TRANSCRIPT - TECHNICALLY OPTIMISTIC - SEASON 2 - EP. 8

RAFFI VO: In June of 2022, almost exactly two years ago, it seemed like the U.S. Congress was on the verge of doing something truly significant. The House subcommittee on Consumer Protection and Commerce had just finished marking up a bill that would finally give the United States a strong, comprehensive federal privacy law. Representative Cathy McMorris Rodgers of Washington state spoke on its importance.

> [**CLIP Rep. CMR from House subcommittee markup 6/23/2022 on the ADPPA, 30:47-30:53; 31:02-31:11**] **Rep. McMorris Rodgers:** *More than eighty percent of Americans support the key pillars of our legislation. Our framework is the best opportunity we've had in decades for a national data privacy standard. It's a culmination of years of effort…*

RAFFI VO: A month later, the full Energy and Commerce committee held a vote. The bill passed — fifty-three to two.

This bill to protect consumers was called the American Data Privacy and Protection Act. The ADPPA. And for such a consequential bill to be recommended out of committee with strong bipartisan support — it seemed like a good sign. Maybe this thing might actually get passed.

BRANDON PUGH: ADPPA was was very unique because it was a sign of compromise and there was strong support really among both parties. Huge support.

RAFFI VO: That's Brandon Pugh, a policy director with the R Street Institute, a nonpartisan think tank.

BRANDON PUGH: I think there was people that would have still liked to have seen continued amendments as it worked its way through, but it's like, you know, it's a continued challenge with Congress.

RAFFI VO: The thing is, the ADPPA never made it to the House floor. Some members seemed unwilling to compromise on certain issues. Others, perhaps, became worried about committing to such a resonant piece of legislation as the November elections grew closer.

And so…it died.

> **[Bell sound]**

But now, two years and one whole Congress later, we've got a new framework for a national data privacy law. And right now, it's back in that same House Committee, being marked up. It's called The American Privacy Rights Act, or APRA.

> **[CLIP Rep. CMR from House subcommittee markup 5/23/2024 on APRA, 2:28-2:48]**
> **Rep. McMorris Rodgers:** *The American Privacy Rights Act gives the power back to the people by equipping them with the knowledge of how their data is being used to monetize, manipulate, and exploit them. This legislation is so important . . .*

RAFFI VO: And that's Representative McMorris Rodgers again. Now, two years later, she's co-sponsoring the APRA along with Senator Maria Cantwell. And as I watch the developments, along with many other privacy heads out there, I'm asking myself: does this one have a shot? Or will it be the same, sad story…all over again?

This season, we explored *many* different reasons why a national data privacy law might be useful. To prevent abuse and surveillance. To mitigate harms to children. To restore some semblance of regulatory authority over big tech companies. So, we're gonna spend a big part of today's episode, our last one this season, talking through this bill.

BRANDON PUGH: It's actually hard to find an American or even a member of Congress that does not care about privacy and largely wants a comprehensive federal privacy law.

RAFFI VO: Brandon's gonna be helpful. But I'll also be speaking with Representative Anna Eshoo of California. She's my representative in Congress, so…that's just good constituent outreach on her part.

And we're not just talking about Congress and regulation. I also want to close our season out with a couple stories — you can call them case studies — about what the future of data, and data collection might look like.

We're also gonna hear from a Hollywood actor from the Marvel Cinematic Universe…no spoilers here…

And…an old friend of mine.

CORY DOCTOROW: I met you back in the napster days Right?

RAFFI VO: That is Cory Doctorow, internet activist, author, blogger, and something of a digital privacy expert. We first met back in the year 2000, when we were talking about peer-to-peer tech, the distributed web, and how to give power to the people. Cory hasn't stopped thinking about that. And this episode, that's what we're talking about, too.

I'm Raffi Krikorian…and from Emerson Collective, this…is Technically Optimistic.

THEME MUSIC

CORY DOCTOROW: You know, Facebook makes a bunch of, uh, extremely unfalsifiable and pseudoscientific claims about hacking our dopamine loops and being evil wizards who built a mind control ray out of big data, right?

RAFFI VO: As a journalist, an activist, and a policy advocate, including with the Electronic Frontier Foundation, Cory has always been keen to distinguish between what's real…and what's just hype.

CORY DOCTOROW: There are some extremely material things that Facebook absolutely does. Facebook spies on us. That spy data feeds into a wider ecosystem of really creepy commercial activity and law enforcement activity. Oppressive governments around the world demand that data. Facebook hands it over to them. Cops use that data to do everything from, like, track people into abortion clinics to round up everyone who shows up at a protest. That data is used to discriminate against people when they borrow money or apply for jobs or apply for apartments or try to get bail. And when we spend all of our energy talking about like the hypothetical evil dopamine hacking wizard, we're not talking about that.

RAFFI VO: At the start of this season, we talked about the term "surveillance capitalism," popularized by author Shoshana Zuboff, professor emerita at Harvard Business school. In Zuboff's narrative, tech companies essentially stumbled upon a "rogue capitalism," as she called it, where new methods of extracting our behavioral data were put to use in order to make new products. Things like predictive algorithms, and artificial intelligence, for example.

CORY DOCTOROW: And, and so, if there's a contrast I have with Zuboff, it's not that, you know, privacy is urgent. I think privacy is very urgent. I think Zuboff is very sincere. I just think that it is very dangerous to take these firms at their word when they make marketing claims.

RAFFI VO: One of the things that Zuboff does say in her book is quote, "If past is prologue, then privacy, data protection, and antitrust laws will not be enough to interrupt surveillance capitalism." End quote. And it's clear that Cory disagrees with this.

CORY DOCTOROW: So, you know, the thing that I think a lot of people who are skeptical of capitalism believe erroneously about the surveillance capitalism hypothesis is that it's anti-capitalist. Zuboff's a business professor at Harvard. She loves capitalism and, and her thesis is when she calls surveillance capitalism a rogue capitalism is that capitalism's magic is that it, it captures information about people's preferences, desires, and willingness to pay.

The thing that makes a company not treat you like the product is if treating you like the product results in something terrible happening to them, like a regulator or a competitor, or even their own workers punishing them. Or better yet, someone makes a privacy blocker. And then instead

of the revenue rising to whatever you thought it was going to rise to, once you started spying on me, the revenue for me drops to zero. Being treated with dignity is not a customer reward program. It's the result of companies fearing what you will do to them if they don't treat you well.

RAFFI: You know, part of the problem is that consumers don't understand the true cost they're paying for things. Like, like all these costs have been made invisible to them. We're extracting data. All these companies value that data, and so they're participating in a market economy that you, Cory, don't know you're, you're participating in, but they're participating in it. And part of my thesis has been that, like, if we can make that visible back to the end user, that might change the dynamic.

CORY DOCTOROW: So that's true, but it's true under conditions of competition. And this is where it's really important to realize how growth goes in Silicon Valley and how unusual it is in the history of American capitalism. Because for most of the history of American capitalism, growth through acquisition and predatory pricing were both illegal. So before Amazon was a e-commerce juggernaut, it just sold books, right? And the way that it grew was not by figuring out how to move into all the other lines of business that it dominates today. It was by buying the companies that had come to define those other verticals. So one after another, they were snapping up these e-commerce companies, the capital markets loved it because it was a bet on monopoly. People talk a lot about how Amazon didn't realize a profit early on. Yeah, of course it didn't. Its investors knew exactly what they were doing. They're trying to corner a market, right?

Google is a company that one quarter of a century ago made an amazing search engine. Their whole ad tech stack — server management, Docs, Maps, you name it, right? These are all acquisitions.

RAFFI: Yeah.

CORY DOCTOROW: So, these companies have extinguished competition. Broadly speaking tech firms are disciplined by competition. They're disciplined by regulation. I met you back in the Napster days, right, and in the Napster days tech was still much bigger than entertainment, but it was getting its ass kicked. And the reason was, seven entertainment companies were putting a hundred tech companies up against the wall. And seven entertainment companies have message discipline. And they have extraordinary profits. Because they divide up the market like the Pope dividing the New World. And they don't compete head to head.

So these companies, the hundred tech companies, they were a rabble. They couldn't agree on what to tell regulators. They couldn't agree on where to hold a meeting to decide what to tell regulators. Tech is now super consolidated. And basically they've cooked up a regulatory regime where any labor right you have, any consumer right you have, any privacy right that you have, they can just violate it and saying, “I didn't break the law because I did it with an app.”

So we don't have any, any regulatory discipline. And then tech is disciplined by interoperability. Because, you know, digital tools are flexible. But one of the things that regulatory capture gets you Is the ability to mobilize IP law against your competitors. So we have this kind of thicket of IP, felony contempt of business model, that makes everything that's not mandatory forbidden. So now we see the tech workforce gutted. We see interoperability on the back foot, regulation dead in the water, and no competition.

So yeah, by all means, tell me how much the real price is, but what does it matter if I can't shop around?

RAFFI: I mean, maybe give me a history lesson for a second. Is there like a point in time that we went wrong?

CORY DOCTOROW: Yeah.

RAFFI: Is there like an original sin somewhere that we should be poking at?

CORY DOCTOROW: Yeah, 100%. The original sin is Reaganomics. And here's the thing. Tech and Reaganomics are perfectly coterminal. So every year that tech existed, antitrust got weaker. So every sector is now as concentrated as tech, right? But tech was first because tech was the sector that grew up at the same time as antitrust was dying.

RAFFI VO: Cory points to the antitrust case against IBM from 1969-1982 as a piece of important history here. It illustrates how resource-intensive antitrust cases can be. There were over 700 trial days that took place over 13 years. But it also shows us how consequential it can be. Even though the government ultimately dropped the case, going after IBM arguably gave us personal computing as we know it today.

CORY DOCTOROW: And they got off the hook, right? But, at the end of it, they were like, God, we don't want to go through that again. So, it's time to build a PC. First thing they do is they say, we're not going to bundle software and hardware. We're going to have a third party OS provider. And Microsoft is born. They say, we're going to use commodity components, right? And the IBM PC clone is born. Gateway, Dell, Compaq, all these companies are born, right? So we get this like, just eruption of competition and innovation even as antitrust is dying, so it kind of masked the effect.

But we missed antitrust. And so that was the original sin. When you're like two guys in a garage in 1985 and you hire your frat buddy who's just graduated with a law degree to be your GC, when you say oh drop a memo for acquiring that other company in a nakedly anti-competitive acquisition, that guy doesn't say don't do that. Don't — especially don't — put it in writing. Oh my god. What are you doing? He's just like yeah, I'll draw that memo up. So you just have this, like, generation of people who come up who think that doing stuff that's totally illegal is fine and normal. It was always going to be the outcome of a world where we don't enforce antitrust. That

was where we were headed. And it was this original sin of technology. And it took us to where we are now. And that's why tech workers are getting laid off. That's why people's privacy is being horribly violated.

When you live in a world in which regulators in the government are clearly in cahoots with large firms to screw you, people who say no no no, everything is fine and the institutions are good and you should trust what they say…sound ridiculous.

RAFFI: So like if the original sin is antitrust, I'm not convinced choice alone brings us to data privacy. Like what else do we need to layer on top of choice?

CORY DOCTOROW: Sound regulation.

RAFFI: Okay, what's that regulation look like then?

CORY DOCTOROW: Okay. So, let's just talk about the state of consumer privacy law in this country. Consumer privacy law in this country was last updated federally in 1988. The law that was passed in 1980 is called the Video Privacy Protection Act. It prohibits video store clerks from telling newspapers which VHS cassettes you take home. Like, three things that don't exist anymore. A lot's happened since then.

RAFFI VO: Cory has a little bit of a wishlist for what he'd like to see in a national data privacy law.

CORY DOCTOROW: So you would say, in general, you need to enumerate every use of data that you collect. You cannot exclude me from a service for refusing data collection. We should have extremely narrow essential purpose exceptions, because otherwise what you get is what we have now, which is the kind of malicious compliance of a million consent boxes. Right, so we do want some consent fatigue, uh, but we want it to be oriented around minimizing collection.

RAFFI VO: Sodoes the APRA framework include all these things? I was curious, so I called my representative in Congress.

REP. ANNA ESHOO: You know, life was much, yeah, life was much simpler when the only thing that was aggravating us to no end were robocalls.

RAFFI VO: Congresswoman Anna Eshoo represents California's 16th district, and that's a noteworthy one when it comes to tech regulation because it includes the likes of Google campus, Tesla headquarters, Stanford University, my house, and a big chunk of Silicon Valley.

REP. ANNA ESHOO: I think that privacy is in the DNA of the American people to begin with, before you ever have any discussion about privacy legislation, what should be in a law, what shouldn't be in a law. It's in our DNA.

RAFFI VO RT: So, if that's true…why hasn't any law passed?

REP. ANNA ESHOO: Because it's hard to do. It's very complicated because you're talking about different systems and there are many stakeholders in it, and what, uh, aggravates the average person can be a great source of income to a company.

RAFFI VO: Before we even take the time to talk about what provisions might be inside this new American Privacy Rights bill, given how our hopes were dashed a couple years ago, it's worth asking: why should we think that the outcome is going to be different this time?

BRANDON PUGH: I think we're all united that we want a privacy law and we want American privacy protected. But, you know, I hate to see some of these provisions would be the hold up and, you know, kick this to the next Congress because it does seem like there is a spirit now to move this ahead.

This is an issue where I see both parties wanting to work together. And it's definitely possible.

RAFFI VO: Okay, so it's possible. Thanks, Brandon.

Actually, Brandon gets right to the heart of the matter. If the APRA is going to have a shot, it's gonna take compromise.

BRANDON PUGH: I think there's many concerns about the draft, but there's also many people that love the draft. If we ever want a federal law that's gonna help most Americans or all Americans, compromise is gonna be key. And I think people are just gonna have to decide how much are they willing to compromise versus, perhaps, sitting around for another decade without a federal law. Meanwhile, states continue to pass laws that are, in my view, a challenge for industry to comply with.

RAFFI VO: In the absence of a federal law, states have taken it upon themselves to pass their own data privacy laws. A lot of them were based on the old ADPPA framework. It's led to a situation that Brandon calls the "patchwork." And it causes a lot of headaches.

BRANDON PUGH: There's definitely members of industry that think that, saying like, the current patchwork and what is quickly even getting worse day by day is not obtainable, or you just can't follow. It's not, it's not reasonable, especially for small, medium sized businesses.

REP. ANNA ESHOO: A lot has changed, Raffi, from two years ago. Sixteen states are now engaged in the privacy business in their state, which really pleases me, and, California, amongst them, is the strongest, the one that has done the most work on this, established an agency, and it's sophisticated, it's broad, it's deep, it really speaks very clearly to consumers in california. And it was the voters. They not only fought to get it on the ballot, and then passed it. So this was highly intentional in California.

BRANDON PUGH: Basically the question is, well, what happens to those state standards and those state laws if there's a federal law? And that's essentially where preemption comes into play.

REP. ANNA ESHOO: Now what's preemption? What it means is the federal government is the only player in it. It doesn't allow the states to say and do anything. Now I'm bringing this down to a very, you know, kind of street level, but I think that it's important for people to understand it that way because that's the way it's going to end up working.

RAFFI VO: Preemption refers to the provision in the APRA that says, no state can make or enforce any state law that would overlap with what's in the federal bill.

REP. ANNA ESHOO: Why do I have issues with preemption?

RAFFI: I was gonna ask.

REP. ANNA ESHOO: What the states have is essentially wiped out. It upends it. And what other states have done as well. A national privacy law does not have to be drawn up at California's cost. Now it's not just California, though. In major, major bills that have become law — the Clean Water Act, the Clean Air Act, civil rights legislation, HIPAA legislation — in all of those major, major laws, the Congress saw fit to allow states to build upon them. So if it makes the the law stronger, improves it, that's allowed. Except in this, it isn't. Is there a need for federal privacy legislation? Absolutely there is. It should be a floor and not a ceiling.

BRANDON PUGH: So you could have a few standards. You could have a federal standard just become the floor, Uh, meaning that states could continue to go farther, or you could have a strongly preemptive standard that essentially would become the one unified standard and state standards would be essentially replaced.

So there is strong preemption, but there's two caveats to that. There are a number of carve outs, essentially areas where states can continue to legislate. Largely around areas not covered by this bill. And there are some that question whether those carve outs may be, like, exploited by states that still want to regulate privacy and are creative, um, and perhaps there actually is not a uniform standard. So that is a, that is an argument that's very much alive right now.

RAFFI VO: And that ambiguity that Brandon's talking about is troubling to some members of Congress. Like Anna Eshoo.

REP. ANNA ESHOO: So, I think that there is a very important, strong case to be made that this language that the draft holds right now be changed.

RAFFI VO: Another provision in APRA is the requirement that certain algorithms be subject to audit before being put on the market. These reviews are called "impact assessments."

BRANDON PUGH: Yeah, so, impact assessments, this is very generalized, but if you're using an algorithm, you essentially have to do some sort of assessment that gives a little more clarity on how that algorithm is being used, how it's being developed and how it's being deployed.

The most recent change would say a certified independent auditor would be the one that could conduct them and when their assessment is done, it goes back to the person that developed the algorithm.

It was tied to specific harms before and now they've Done a new definition of consequential decisions. So if you're using an algorithm and furtherance of a decision around housing, employment, credit, healthcare, et cetera, those are consequential decisions. I haven't counted exactly the number of them.

There's been a lot of proposals both ways though, in terms of how we, we could sharpen this to get at, um, a smaller class of consequential decisions. But there are just as many proposals that seek to make it broader, and think maybe the definition is too narrow.

RAFFI VO: Under the bill, some of these impact assessments would be subject to government oversight, via the National Telecommunications and Information Administration…the NTIA. An agency you've probably never heard of.

And Congresswoman Eshoo has a bone to pick with that because she worries that another agency has been inappropriately sidelined here.

REP. ANNA ESHOO: I think that the authority of the FCC is being undermined in the bill. This is, this is the agency that has the expertise. And if you upend that expertise in the FCC, you're not going to, it can't, it's not going to be recaptured.

RAFFI VO: Also in the APRA, a stab at regulating data brokers.

BRANDON PUGH: Data brokers have been a topic of conversation now for a while. So what this bill is seeking to do is have a more holistic approach.

So on one end you're going to have a registry, so data brokers that meet the definition would have to register. And as part of that registry, there would be a do not collect option essentially somebody could go and say you know I no longer want you to collect without my consent. You'd also have a delete my data Option which essentially means that data on an individual that they did not directly collect would have to be deleted. I believe the time frame for that was within 30 days. There are some exceptions to that realizing that maybe there's some legitimate law enforcement purposes for this, because there is a fear out there that, you know, perhaps criminals would use this as a way to delete their data. And that's the benefit of a law like this is that as a consumer, you are now going to be empowered to have rights around your data in terms of how it's collected, how it's transferred, how it's sold.

REP. ANNA ESHOO: Data brokers. I mean, what an operation. Raffi, it's jaw dropping.

Raffi: Jaw dropping.

REP. ANNA ESHOO: It's jaw dropping. Now, California set the gold standardfor dealing with data brokers. The DELETE Act gives consumers the right to stop data brokers from collecting their data and then selling it.

RAFFI VO: So, it remains to be seen how the final version of the APRA would measure up against the California law, in terms of an individual's right to have their data deleted. But it's clear that implementing some version of this on a national level would be a big deal. Kind of like it was for the Europeans, when this was included in the GDPR.

CORY DOCTOROW: So, I think that a sound privacy law would look a lot like the GDPR but better enforced.

RAFFI VO: The GDPR is the EU's big data privacy law, which went into effect in 2018. As we talked about before, it's the reason why you get annoying pop-ups asking which cookies you want to accept.

But it also does a ton of other things, like implement strict consent requirements, and gives consumers a right to export their data. But it's a big, complicated bill, with lots of intricacies.

BRANDON PUGH: I would not want to see a GDPR implemented in the United States.

RAFFI VO: BRANDON PUGH of the R Street Institute.

BRANDON PUGH: And it's hard for an American to critique these things because we largely have done nothing in any of those spaces. There are a lot of provisions that are burdensome to business and that in my view have not struck the right balance between balancing consumer privacy, innovation, um, and security. I think they've tipped too far in certain directions in certain

areas and just You know, at times like needless bureaucracy. It's just not the view that U S traditionally has had. Whereas that obviously is the view that the European union has had.

RAFFI VO: But CORY DOCTOROW is all for it. Though the GDPR might have led to a lot of long, bureaucratic consent agreements that are a pain to read, if the law works properly, you really wouldn't haFF to read them. I mean I know no one's reading them anyway, but…imagine if it didn't matter!

CORY DOCTOROW: One of the arguments that large tech firms make is that they defend you from privacy threats. And they absolutely do, right? They are in a position of irreconcilable conflict of interest when it comes to your privacy. They want you to have privacy from everyone except them.

So long as the floor is a regulation that says, you can't process my data without consent, and you can't sell it, and you can't do all these other things with it, you don't have to read those privacy policies, right?

RAFFI: Yeah. There's no "gotchas."

CORY DOCTOROW: Yeah.We could get to a world where we don't have to read it because it doesn't matter. Because, like, they're just not allowed to hurt you.

RAFFI VO: One way to be sure that these companies couldn't hurt us would be to put a stop to targeted advertising. And the APRA framework does take some steps in that direction… with a few notable exceptions.

BRANDON PUGH: All ads aren't targeted. Like there's a difference between first party ads versus contextual ads. Like those definitions really matter. And those definitions changed in this discussion draft. So there is a permitted purpose for targeted ads, which means that the text alone says that you can do targeted ads. You can't do targeted ads if it's using sensitive data, which is a huge difference. It has to also be data previously collected. But you can opt out though. So if you're a consumer, there still is an opportunity for you to say, you know what? I don't want targeted ads. And I think that's where some of the concerns, especially among the ad

RAFFI: Does your framework then preclude surveillance advertising? Or do we need to say that in addition?

CORY DOCTOROW: No, no. Surveillance advertising, we should extinguish it entirely.

RAFFI VO: CORY DOCTOROW again.

CORY DOCTOROW: There's a lot of good reasons to do it. Like the surveillance advertising pipeline feeds all these other harmful uses, doxing, and stalking. But also we should ban it to save the news.The ad tech sector today takes 51 cents out of every ad dollar. And the reason for that, to a first approximation, is because tech companies will always know more about the user of a publisher's website than the publisher ever can.

Now the alternative to surveillance advertising is context advertising based on the content of the article. And the publisher always knows more about the content of the article than the tech company. So we're talking about hundreds of millions more opportunities to show people ads. If you have a meaningful privacy regime, if they're context ads. So there's a lot of ways that surveillance advertising is really bad for publishing. And, you know, getting rid of surveillance ads would really go a long way to fixing it.

RAFFI VO: But BRANDON PUGH sees things a little differently.

BRANDON PUGH: I think to give you a concrete example, you know, permitted purposes under the bill, which essentially means it falls under data minimization, is we're going to restrict the amount of data that can be collected.

There are some concerns whether that list is actually complete. So would there be a purpose that we're not contemplating right now or a purpose that's needed for advertisements that's not reflected and that could, you know, uh, inadvertently impact the ad ecosystem?

As it stands, uh, there are 16 permitted purposes. So, uh, generally speaking, you would have to fall under one of those 16 permitted purposes to be able to collect and use the data.

RAFFI VO: Those 16 purposes listed in the bill include things like: to protect data security, to comply with law enforcement, and to investigate harassment. But there are also weirder, vaguer ones, like: to conduct market research, to transfer assets to a third party in the event of a merger, and, actually, one of the stated reasons is to “provide targeted advertising,” for individuals who don’t opt out.

BRANDON PUGH: There is that first provision that essentially is if you're targeting it for a product or service requested, but outside of that there'd have to be a permitted purpose. I think the concern is there you may have a legitimate use of data that does not fall under within one of those 16 permitted purposes, you know, so there's some talk whether there could be a catch all or some sort of way as a relief valve or a way for the FTC to do rulemaking on that front.

RAFFI VO: And then, there’s the big one. The private right of action.

CORY DOCTOROW: And then the final thing that we need is a private right of action. This is where it always goes wrong because the Chamber of Commerce hates this, but the private right

of action is the right of you to sue over violations instead of relying on solicitor general or attorney general, or your city attorney to decide that what happened to you rises to the level of doing something.

RAFFI VO: But, BRANDON PUGH has a different take.

BRANDON PUGH: I'd say the reason the private right of action is so controversial is there is a concern that, you know, maybe attorneys or individuals themselves may exploit it for financial gain rather than going after, you know, legitimate privacy harms. Because I think most people probably agree if you intentionally commit a violation here just, you know, for profit reasons, that's different from somebody that maybe it was inadvertent and now a consumer saying, gotcha, I'm suing you. Not to make it oversimplified. So there is definitely, I think that concern with the private right of action. However, it has become part of the delicate balance. You know, maybe I'll be wrong, but it's hard to imagine the federal privacy law that may not have a private right of action.

Not saying that that is, you know, great. But I just think that's kind of where a lot of the compromising consensus has has panned out.

RAFFI VO: But Cory is far less worried about the possibility of gaming the system here, and, as usual, is more concerned with making sure people's needs are actually met. And besides, there's precedent for a private right of action working out just fine.

CORY DOCTOROW: And an example of this would be the Americans with Disabilities Act. It's self enforcing because every grievance from a firm that refuses to comply with ADA is a monetizable event for lawyers. This is actually an area where markets work pretty good.

RAFFI VO: So a quick recap: the APRA framework could potentially put serious limits on targeted advertising and data brokers. It could potentially lead to more transparency around algorithms. It could disqualify some of the most ambitious state privacy laws, but it would safeguard an individual's right to sue companies that violate the law.

There's lots more in the APRA that we didn't get to. And remember, as we covered in a previous episode, the current draft also includes provisions from the bill formerly known as COPPA 2.0 to make specific protections for children.

So, if lawmakers want to pursue this bill, the next step would be markup by the full House Energy and Commerce Committee. And that might happen later this summer. But, there's also recent reporting from Axios that House Republicans are starting to get cold feet.

So, I asked BRANDON PUGH: does this thing have legs, or are we about to get burned again?

BRANDON PUGH: I think it'll be a question of, you know, is there time to get enough consensus around it? And we can we move it ahead in both chambers?

RAFFI VO: BRANDON PUGH isn't making predictions just yet.

BRANDON PUGH: I do think regardless and I, you know, I hope a privacy bill passes this Congress. That's, that's my hope. I think we've talked about it too long. If nothing else, though, I do think this is probably where a future Congress would consider starting. And if it's not a future Congress, I do think states, It's just like we saw with ADPPA, we'll probably take aspects of this and consider implementing it at state level, because I don't think the states are going to ease up.

Even among industry, there's not a universal consensus between like what provisions are doable, which are not. I've heard some that say, this is great, let's pass it today. And I've heard some saying, this is not good. It needs further work, but we're committed to getting that done.

RAFFI VO: I asked Congresswoman Eshoo if she'd spoken to any of her more…powerful constituents from the tech giants about these issues. And she said, yes, they've spoken.

REP. ANNA ESHOO: Look, you know, we're, we're grownups, we're adults, we know one another, we respect each other. But these are corrections in the systems that I think are really needed. Actually, I think that they end up with a much better reputation.

RAFFI: This is actually my bigger question, Congresswoman. How do we get more regular people to care? Like when I talk to people about this, it's like some version of, well, Google has it anyway. TikTok has it anyway. Or…

REP. ANNA ESHOO: You know what it is, Raffi? People, out of their frustration over all the years, where there has been more and more and more that's upsetting to people, they know they don't have control over it. That's what they're saying to you. I give up. If you give people, you let people know they have control, and all they have to do is press a button and delete it. They'll say, you know what? Whomever did that, as my mother would say, God bless you. You know? I'm not trying to put anybody out of business. But I've come to question the business models because they have hurt people. So, uh, why not try like hell to do it? It's worth it.

RAFFI VO: BRANDON PUGH agrees and actually, he makes a point that we're always trying to make on this show. In a very real way the power to shape this national data privacy bill…is in your hands.

BRANDON PUGH: You know, it's easy to kind of critique where we're at with this bill. And if you, but if there's somebody listening and they have better solutions or ideas, you know, I think you 100 percent should be submitting them.

Like it's impossible for everybody to be experts in every single aspect of this bill. Many of the changes they made between the discussion drafts were a direct reflection of some of the feedback.

RAFFI VO: Coming up, I get to talk to a movie star about biometric data privacy. And I'll talk with Amy Bach, whose organization sees data as the first step to criminal justice reform.

It's two different case studies for what the future of data might look like. After a short break.

MIDROLL

RAFFI VO: Welcome back to Technically Optimistic. I'm Raffi Krikorian.

I might have mentioned, last October, I was asked to testify before Congress about data privacy.

> **[CLIP of Raffi before House Subcommittee, 10/18/2023, 21:18-21:24] Raffi:** *So I'd like to start with a very simple fact. We live in an age of rapidly increasing digital surveillance, and very few people. . . .*

RAFFI VO: And that's not even my biggest humble brag. While I was testifying before Congress, I also got to meet a movie star.

> **[CLIP of Clark before House Subcommittee, 10/18/2023, 31:04-31:05; 31:13-31:17; 31:24-31:33]**
> **Chair Bilirakis:** *By the way, I'm a fan. You're recognized, sir, for your five minutes.*
> **Clark Gregg:** *Thank you very much. For me it's a great honor to appear before this important committee. My name is CLARK GREGG, as you said, I'm an actor, I'm a screenwriter, I'm a proud member of SAG-AFTRA and of the Writers' Guild. . .*

RAFFI VO: Clark Gregg has been a TV and film actor for decades. And maybe, depending on how old you are, you might know him from The West Wing, where he played FBI agent Casper, or from the MCU, where he played S.H.I.E.L.D. agent Phillip Colson for 13 years.

> **[CLIP of Clark before House Subcommittee, 10/18/2023, 32:13-32:18; 32:30-32:38]**
> **CLARK GREGG:** *I'm here because this issue's been top of mind this year for my fellow writers and SAG-AFTRA members. Actors, like anyone else, deserve to have their biometric information protected from unauthorized access and use.*

CLARK GREGG: We met recently in Washington where we were talking about the Data Privacy Act and I had been asked by my union to show up there and talk about how the Data Privacy Act was useful to people in my position because of the ability to own one's voice, likeness, eye scan, face scan, that would really help us.

RAFFI VO: In the summer of 2023, Clark went on strike with the Screen Actors' Guild. He's a screenwriter too, and so he'd also been on strike with the Writers' Guild. And one of the central issues that both unions were fighting for was better protections for their members in the face of artificial intelligence.

CLARK GREGG: In the same way that writers were trying to maintain that they themselves are something different than AI, that they have an ability to copyright and have authorship in a way that a computer does not. We're trying to say that our face, our likeness, our voice, our, you know, whatever we call our personality belongs to us.

RAFFI VO: He told me about a shocking provision that the studios included in one of their proposed contracts, one the union did NOT accept.

CLARK GREGG: We received something called a last, best and final offer. And what was in there was the idea that anyone who worked above minimum, a very large majority of employed actors, they would be scanned and that their likeness could be used in the future without consent, and that they could even be used after the person was deceased. And frankly, this caught quite a bit of instantaneous blowback.

RAFFI: Even just making an offer that starts with "even after your death" seems crazy.

CLARK GREGG: Look, I can be naive when it comes to business. Sometimes many people who work in the arts, we're told that we are being naive. But I would say that many of the people that I've spoken to, who are writers, actors, or directors, while we have close friends who work in those companies, we're kind of flabbergasted that there is less of a, let's just say, kind of departure point of respect and partnership. Like, why would you even put that in there?

RAFFI: Yeah.

CLARK GREGG: I mean, you know, a business person would say, like, hey, it can't hurt to ask, but it does kind of hurt when you ask that because it really erodes trust. It seems especially present in this moment in capitalism, which is the profit drives the decision. And I think that's not bearing out to be necessarily that good for human people. It needs to be tempered somehow and that should no longer be looked at as some kind of anti-business, anti-capitalist, but pro-human idea. You know, we're just the Actor's Union for God's sake. There's not that many of us. And the funny thing is that all of us have spent time watching or working on dystopian sci-fi things where these are all the early beats of the, pretty soon we end up as human batteries or running away from the hunter killer robots. This is all very familiar to people who love sci-fi. The idea that we're going to just, for the sake of profit, for the sake of profit for corporations, as opposed to profit for people, we're going to turn ourselves into a bunch of zeros and ones. It almost feels like, okay, it's the matrix, but we're deliberately climbing into the canisters and plugging ourselves in. And I've talked about this, because I've been scanned a bunch.

RAFFI VO: Clark talked about being scanned in his testimony to Congress.

> **[CLIP of Clark before House Subcommittee, 10/18/2023, 33:13-33:47] CLARK GREGG:** *Like any performer in a Marvel, or any visual effects-driven film, I've been scanned. I've been scanned many times. You step into a tiny dome where there's literally hundreds of cameras, they record every detail and angle of you, and they create something called a digital double, which scared me ten years ago; it really scares me now. This can be used with your voice, either real or synthesized, to recreate your character, to create a new character, or, in the wrong hands, ironically, as you said, Chairman Bilirakis, a bad actor, it can create a new you that can roam the internet wreaking havoc in perpetuity.*

RAFFI VO: When SAG-AFTRA and the studios finally agreed to a deal in November of last year, the agreement contained a few landmark provisions for how to treat the products of AI.

The contract talks about what they term "synthetic performers," digital creations of AI that appear onscreen and then, there's "digital replicas," digital creations of AI that appear onscreen but have been deliberately designed to replicate a real, working human. And the good news is that, for both categories, SAG-AFTRA's new bargaining agreement specifies that human actors have to first give their explicit consent.

And this is something that Clark was hoping for. Because, as an actor, your likeness is more than just your livelihood.

CLARK GREGG: You know, one thing you learn when you're an actor is that some of the performances you do, especially if they're good, they really influence the way people see you. I played a pretty a pretty aggressive zookeeper in a movie called Mr. Popper's Penguins, who was trying to kidnap some cute baby owls. And I got to tell you, when I walked into my daughter's fifth grade class to read for them, there was some very unfriendly looks.

RAFFI: When was the first time you saw yourself deep faked somewhere? I'm just curious about that experience.

CLARK GREGG: Um. I think the first time, I may have unfortunately mentioned this in Congress, you know, people sent me some comically obvious Photoshop's of me in a pornographic images. I'm not prepared for the moving version of that. But then there was also a VFX driven television show I was working on where there was some stunts that I was very happy to not be doing, a car flying off the roof of a building. And there was definitely a digitally enhanced and/or rendered version of me in the car falling. And you know, I didn't stop frame it, but the moments you could see like, okay, that kind of looks like me, or that kind of doesn't.

RAFFI VO: And you don’t have to be in the movies to know that unsettling feeling. If you’ve messed around with generative AI tools to spawn an image of you or make a clone of your voice or even, if you’ve asked a chatbot to write something in your style, you might end up in a similar place as CLARK GREGG did.

CLARK GREGG: There are consequences to technology. And I was on a panel the other day with a couple of young gentlemen who were involved with AI and developments of it, and they were very, in my mind, too circumspect. Adapt or die, is what one of them said. And I was like, okay. I mean, I hear you, but what you have to then consider is what's driving the adaptation. There is an endpoint and there is a driving force. And is that driving force, again, prioritized around profit or the betterment of humankind? And are you sure that they're exactly the same?

RAFFI VO: So this is case study number one, and a vision of a future where surveillance capitalism is fully in control. If our digital behavioral data was the new frontier that enabled surveillance capitalism in the first place then our biometric data might be the next frontier. Your likeness, voice, and even more could all be up for grabs in the same way that your GPS data and purchase history are now.

This version of the future is pretty bleak, obviously. But it does represent the endgame of a certain “adapt or die” attitude that we can already see being adopted in the tech world.

But I also spoke with AMY BACH, the founder and executive director of an organization called Measures for Justice. And, look, most of the talking about “data” that we’ve done this season has been around personal, digital data. The electronic footprint of our online lives. Amy’s whole world is data, but in a more old-school sense.

AMY BACH: if I asked you where the good public schools are where you live, you could tell me. And you know that because there are teacher student ratios, test scores, college admissions, all sorts of things, right? And if I said to you, Where's the good hospital? You would be able to sort of say, if you're having a baby, you go here, if you need a neurologist, you go there. If you have cancer, this one. And the reason is because we have measures for these, all sorts of things, like doctor patient handoff rates, survival rates, all sorts of things. Now, if I said to you, how does your criminal justice system operate and how does where you live, compared to the other counties around you or the other places across the country, most people would have absolutely no idea.

And the problem is that in America we measure everything. We measure our hospitals, we measure our schools, our water supply, our sports, everything really except our criminal justice system. The people who experience the criminal justice system don't form constituencies in the same way that parents do for schools or patients do for hospitals. People haven't understood what it could mean to have a transparent, accessible and accountable system.

RAFFI: So, on one hand, data is power. But then, two, I guess, like, I'm curious, what systemic reasons are there for that data not to exist in the first place?

AMY BACH: Yeah, I want to address one thing that you just said that data is power. Okay. That is so true. And our motto is “no data, no change.” And the fact that it is power is one of the reasons why .the people who are in charge of it have really tried to shield it. So it's collected by prosecutors, by courts, police departments, and the data is collected for administrative purposes. And all of this information is not created for data analytics, but it's created for the daily use of what happens in a court.

RAFFI VO: The data that Amy is interested in is kept and collected without much regard for how to organize it. Records have to be kept, by law, but there’s little to no oversight as to how it’s structured. And this can lead to errors and omissions, and disarray.

AMY BACH: What my organization does a lot of times is to take this administrative data and get it from an agency, which is hard in itself, right? First, you've got the agency, like prosecutors and police, and we ask for it, and many times it's missing years, missing data elements, you know? And the thing is, we've never seen really a good data set.

RAFFI VO: And they’ve seen some truly wild and scary things.

AMY BACH: We have this one state, and internally we had a joke that every person was born a crime. And that's because every person's crime was listed the date as their birthday. They had all the missing dates in an entire very, very important state.

RAFFI: Whoa.

AMY BACH: And we had to fix all of that.

RAFFI VO: And because we’re talking about the criminal justice system, a dataset that represents how communities police and judge and sentence their members, the problems here aren’t just about bad data hygiene. It’s about the ramifications of bad record-keeping on the rule of law. It’s about how bad data can lead to a failure to protect people.

AMY BACH: I think that in order to make the data decent, you have to use it. Right? And, no one's keeping track of whether it's good or not. So in the Mississippi Delta, I met this woman, and she'd been beaten up horribly by her boyfriend with a tire iron, and her case was never prosecuted. So then I went back to that court clerk, and I said, When was the last time a domestic violence case was prosecuted? And she said, you know, she looked in her little crappy computer and then she looked back in these big bound volumes and she said, there hasn't been one prosecuted in 21 years. They're not looking at patterns. In this county, they kept their data on a steno pad. This is not uncommon in America.

Raffi: But then how do you make, I mean, I know the answer to this question, but like, how do you make policy decisions then if this is what we're dealing with?

AMY BACH: That's the question, right? So we've got to go in and clean it and code it.

RAFFI VO: The first step is acquiring, and evaluating data from local agencies. Once Amy sees what they're collecting, not collecting, and how the goal is to come up with a set of data collection standards.

AMY BACH: Like, people really didn't want to be measured. We created legislation and a series of standards, And basically, it says what every court should collect and how you should collect it. And what you can see very quickly, um, when, you know, when they start being measured publicly is that the number of felonies go up from, you know, right away.

RAFFI VO: After making standards for collection, the next step is standards for organizing the data. That means creating a structure or "schema."

AMY BACH: The data is basically raw and we've reclassified it to make it into the standard schema, right? And we have a data dictionary that we use across the country, which makes the measures from different jurisdictions comparable.

RAFFI VO: Let's think about how Amy's project connects to data privacy.

On the one hand, this is a situation where data is being kept *from* us, even if not deliberately. But really, this is about differing opinions on what's important.

In the quest for cleaner, standardized data, is there a risk that we're imposing some categories that don't always make sense? Is there such a thing as *too much* transparency?

AMY BACH: Yeah. That's such a great, I mean, would you want transparency? Like, Raffi, if I said to you, like, someone's going to follow you around all day.

RAFFI: Yeah. No. Absolutely not.

AMY BACH: And write about what you do and they're going to, you know, see what you click and what you don't, I mean, you would be like, no. So, I mean, too much transparency? I think, um, there is.

RAFFI: I guess like maybe what I'm asking is like…

AMY BACH: Yeah, what are you thinking about?

RAFFI: I'm trying to figure out whether transparency and privacy are coming into collision somewhere.

AMY BACH: Yes, that's what I thought you were thinking about.

RAFFI: Are we trading off societal transparency for individual lack of privacy. There's a trade off here that I'm trying to understand.

AMY BACH: Can I tell you what I was thinking of when, when you said that?

RAFFI: Please.

AMY BACH:I was thinking of all the terrible predictive analytics, like, figuring out what someone's risk score is, like a defendant's risk score is in committing a crime again. How you could do that on the data that we have, that's a crime, okay? Because I've seen the data in there. There's no way it's good enough. So I feel like that, to me, it's like a fake transparency.

RAFFI: What's your endgame then? Like, is your endgame that we have standardized all this data across all, I don't even know how many counties there are in the U.S., but like…

AMY BACH: 3,124.

RAFFI: Okay, that many counties. Is the endgame that we've standardized all of them?

AMY BACH: My proximate end game is to change the culture so that people in America can see what's going on in their justice systems and hold it accountable, that they're in dialogue with their justice systems to make them be better. And it's not operating in a black box. But the ultimate is that all of the data, the prosecutor data, the police data, the sheriff data, the court data and ultimately, the Department of Corrections data, which is, you know, probation, parole, that it's all, it's not in silos, it's connected, and It's not being used in harmful ways, but it's being used to change and protect people who need it most. Like, that's it.

RAFFI VO: So this is case study number two. And it’s a vision of the future where we accept Amy’s goals as our own. Our data does not have to be only the raw material for private corporations. Our data can be used to serve our interests.

And like I said, I know there’s a difference between the digital personal information we store on our phones, and the aggregate criminal justice statistics from America’s 3,124 counties. But the lesson here is about overcoming the institutions who want to keep our data entrenched in the status quo.

And that applies just as much to all the local agencies with their own little systems for organizing crime data as it does to all the big tech giants with their own proprietary models, fed by data they've extracted from you. In this version of the future, those trade secrets are nullified because we can do the hard work of taking our data back and making it work for us.

That's what Amy did. And, if we were to build a coalition around data privacy, that's what we could do, too.

In my conversation with CORY DOCTOROW, I asked him a question along these lines.

Raffi: Maybe, is the right way to look at this, like, what do I, Raffi, you, Cory, deserve? Like, is that the way to look at it?

CORY DOCTOROW: Sure, I think I have a short answer for it but you deserve technological self determination.

RAFFI: Okay, but what's that mean?

CORY DOCTOROW: So what it means is, you deserve to have a say in how the technology that you rely on works. And so that say can arise from many different things.

Maybe there are so many well described products in an orderly marketplace that you can just find the thing that works the way that you want it. Maybe there's so many aftermarket add ons that you can get the closest thing and adapt it. Maybe there's a regulator that steps in when a firm does something untoward. And stops the company from doing it.

You know, I have, uh, some, in the grand scoop of things, relatively minor disabilities. I have a vision disability that makes it hard for me to read low contrast type, and how my technology works makes a huge difference. Like, there's a lot of type I can't read.

RAFFI: Sure.

CORY DOCTOROW: Unless I can change the type, right? And so I have a lot of appreciation for technologists who thoughtfully try to approach my needs. But the second you say you've met all my needs, including the needs that even I haven't thought of yet, and you have closed the device so that I can't adapt it to my needs. That's when we stop being friends. That's when you're my enemy. That's the rock bottom of a failure for technological self-determination.

RAFFI VO RT: So it seems like one way toward technological self-determination might be through prioritizing open source software. Or, you know let's unpack the phrase "free

and open source" maybe not just open source, where users have access to the code, but also free, like in terms of freedom, where people could go and make whatever changes they want, and do whatever they want with it.

CORY DOCTOROW: You know, they were supposed to be the same. And they were at first, right? Open source and free software were the same. The thing is, that open source was an instrumental account of what the license was doing. It made the software better. You could review it, you could understand what it was doing, you had some transparency.

Whereas free software made an ethical proposition of a technological self determination. It gave you freedom. And so then we go down this series of junctures where we're like, What should we do? What is the open or free way to proceed here. And we get to those junctures because open beat free. You have all the openness you want, but you don't have any freedom. Every app we, we make loops through the cloud and you cannot reconfigure the cloud. Only Google, Facebook, Microsoft, Oracle, and so on, they can reconfigure the cloud. They have freedom. We have openness. Is openness good? Yeah. Transparency is good. Transparency is better than opacity. Openness is better than closed, but free is better than open.

RAFFI VO RT: There's some movement in Congress about all this, there's a new draft framework for like a comprehensive data privacy bill. Cory like when you hear news about that stuff…does it make you hopeful?

CORY DOCTOROW: Yeah, yeah, no, I'm super hopeful. We've never been in a moment better for privacy in generations. The coalition for privacy right now, it hasn't coalesced, but it will, and it's everybody who's got something that they're upset about that has some nexus with this very bad privacy landscape that we inhabit.

So if you're worried that like, Facebook made Grampy into a QAnon, or if you're worried about deepfake porn, or if you're worried about algorithmic discrimination for hiring or whatever, you're worried about privacy. And right now, on privacy, we have these coalitions of people who care about all these different issues that cross a lot of political boundaries. Nevertheless, we all care about the same thing. When you understand that the thing that we care about is privacy. I think we're in better shape for a new muscular privacy law than at any time in my lifetime.

RAFFI VO: And that's really good news. And I'm not just saying that because we're a podcast that just finished a season on data privacy. I'm saying that because I want the best version of the future for all of us.

And that doesn't mean a future with less technology. It means a future where more of an effort is made to make sure that the tech we have benefits us. People. A future where the efforts of government and industry reflect the fact that we value humanity more than we value profits.

And look, I'm not saying that all tech companies are bad. But they don't get to decide the future alone. We have a say in the future of data privacy. But that means we're gonna have to make sure our voices stay heard.

I think it's possible. And hey, like we were just saying, there's no better time than right now to put this to the test.

CREDITS:

Technically Optimistic is produced by Emerson Collective, with original music by Mattie Safer. Production assistance from Christine Muhlke. Our senior producer is Erikk Geannikis.

If you've enjoyed the podcast, please rate and review us. That's the end of Season 2, but stay subscribed for updates about what's next for the show.

And sign up for the Technically Optimistic newsletter! You'll get my thoughts about the week in tech, with lots of big questions, interesting links, and ways for us to keep the conversation going. Subscribe for free at technicallyoptimistic.substack.com.

I'm Raffi Krikorian. Thanks so much for listening.