Episode #951: Privacy Primer: A History of U.S. Consumer Privacy, U.S. Federal Privacy Debates, & XR Privacy Implications with Joseph Jerome

October 7, 2020

Kent Bye: The Voices of VR Podcast.

Hello, my name is Kent Bye, and welcome to the Voices of VR Podcast. Privacy is a topic that I've been covering here on the Voices of VR, because I think there's so many different implications when it comes to virtual and augmented reality technologies for what's that's going to mean with our data and who has access to it? And I've always had this issue with companies like Facebook, where they basically say, "Well, our concept of privacy is we're going to tell you what we're going to record. And as long as we tell you, and as long as you consent, then everything's cool."

I always wondered, "What philosophy of privacy that is based upon?" And it turns out that that goes way back to like 1973, and eventually the Federal Trade Commission and this whole history and evolution of privacy, privacy policies, consumer privacy, government surveillance, and privacy from governments. I mean, there's a lot of complications when it comes to looking at the United States law when it comes to privacy. it's extremely fragmented, very piecemeal, very narrowly-scoped. And there's a lot of discussion that's happening right now for the need for a Federal Privacy Law, especially in the light of the GDPR, which came up with a much more comprehensive framework around privacy that can be built upon. In the United States, we don't necessarily have that, and so there's a threat that the United States is going to fall behind, unless we come up with some federal privacy policy law that tries to give a little bit more coherent approach for how the United States government, as well as companies face different issues of consumer privacy.

So today's an epic conversation with Joseph Jerome, he's a privacy professional who's been working on federal privacy policies and legislation for over seven years now, and has taken in a little bit of a interest within virtual reality starting to talk a little bit about some of the privacy implications. He gives me an epic history of the evolution of privacy policy with the United States, and just with 90 minutes gives a great overview. And I actually went through and made footnotes, and over 150 footnotes so that if you want to deep dive and to dig into the evolution of privacy policy, there's going to be lots of different links that you can go and just dig into. But I think this is a good primer to just get up to speed as to what's happening, and some of the different debates and discussions that are happening around a federal privacy law here in the United States.

And just as another point of why this is important for if you don't live in United States, is that a lot of these major technology companies are based here in the United States, and so there are practices that they have by default, unless they're abiding by the regulations of your local jurisdiction, more likely than not, then whatever the U S privacy law is going to be dictating what they do also internationally, just as a kind of baseline. How that actually gets sorted out, the different compliance officers and privacy folks at Facebook have to sort that out. But anyway, this is an epic conversation, and we'll give you up to speed as to some of the discussions that are happening at the policy level, when it comes to privacy.

So that's what we're covering on today's episode of the Voices of VR podcast. So this interview with Joseph Jerome happened on Wednesday, September 23rd, 2020.

So with that, let's go ahead and dive right in.

Joe Jerome: Hi, my name is Joseph Jerome. I'm a privacy and cybersecurity attorney based in Washington DC. My day job is I lead multi-state advocacy work for Common Sense Media, which is a national nonprofit that works to provide independent research and advocacy on behalf of kids and families. We do a lot of work to try to improve the digital wellbeing of kids and students in our increasingly online digital world. Again, I'm also a privacy person first and foremost. I've bounced around working in private practice at a law firm to civil society on a couple of different privacy projects. So I've been immersed in the federal privacy debate for about seven years now. And increasingly over the past couple of years, I've been trying to pay a little bit more attention to emerging immersive technologies and XR. My reasoning for this is multifaceted. I'm a video gamer. I bought a $25 Virtual Boy on clearance from Electronics Boutique back in 1996. And I really think as a privacy person, and we should talk about this, we have messed up or not really done a good job of dealing with data privacy online, in the emerging Internet of Things, and I really think immersive technologies is another opportunity for us to really start from scratch and come up with a better framework that addresses privacy and personal autonomy.

Bye: Yeah, no, I think it's great, just because, well there seems to be a lot of motion and momentum right now towards a federal privacy law. Maybe you could just-

Jerome: I'm a bit cynical on that.

Bye: Okay. Well, I know there's been a number of different legislations and laws, and I want to dive into the VR specific things, but first let's maybe take a step back – and maybe we should go back even further, what is privacy?

Jerome: Oh no, and I know you've mentioned this often. We do not have a shared definition of privacy, that is clear. I think we're a good place to start, and I come at all of this stuff as a lawyer first, which I think clouds my judgment. Sometimes it makes me think about things very technically as a matter of law

and statutes.

I think it might be useful to your listeners to understand the history of data privacy in the United States. And this goes back to 1973, actually in the aftermath of Watergate and a lot of surveillance issues, there was a lot of interest in agitation in the federal government to think about privacy. And in 1973, the Health Education and Welfare Agency came out with a report that discussed privacy, "The State of Automated Systems" in the United States.[1] And that report was what established what is now known as the Fair Information Practice Principles.[2] So everything that's the foundation, or the bedrock of privacy laws in the United States, as well as in Europe, all come from this 1973 report.

And this report talks about how there should be no secret systems and that people should be given access. And that everyone should be disclosing how they're going to be using information, and ensuring it's correct. Everything that we think about in privacy laws originates here. And what happened I think – it's interesting – is that that report recommended that we create a United States privacy law, and we eventually created, what's known as the Privacy Act,[3] but that only applies to government agencies. It didn't cover the private sector. We can surmise why that happened, lobbying or not wanting to stifle 1970s innovation. But as a result, the United States went down this road of approaching privacy in a real piecemeal way.

So we would do privacy laws that impact cable companies. After a Supreme Court nominees video rental records were revealed by to a reporter, we did video privacy rules for Blockbuster,[4] [5] which is totally irrelevant. Now we eventually got to things like health privacy,[6] and financial privacy,[7] and education privacy,[8] but we never did everything that was comprehensive, and so there are gaps all over the place. And to get to your question, the road that we're on now emerged in the late 1990s. The Clinton administration was trying to figure out this internet thing, and the US Federal Trade Commission was charged to produce

[1] U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records,Computers, and the Rights of Citizens viii (July 25, 1973). https://www.justice.gov/opcl/docs/rec-com-rights.pdf

[2] The Code of Fair Information Practices. [Originlly written on July25, 1973]. Retrieved from https://epic.org/privacy/consumer/code_fair_info.html

[3] The Privacy Act of 1974 (Pub. L. 93–579, 88 Stat. 1896, 5 U.S.C. §552a, enacted December 31, 1974). https://www.justice.gov/opcl/privacy-act-1974

[4] The Video Privacy Protection Act of 1988 (VPPA) (Pub. L. 100–618;102 Stat. 3195, 18 U.S.C. § 2710, enacted Nov. 5, 1988). https://epic.org/privacy/vppa/

[5] 18 U.S. Code §2710. Wrongful disclosure of video tape rental or salerecords. https://www.law.cornell.edu/uscode/text/18/2710

[6] Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104–191; 110 Stat. 1936, enacted Aug. 21, 1996). https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[7] The Right to Financial Privacy Act of 1978 (RFPA) (Pub. L. No.95-630; 92 Stat. 3741, enacted September 10, 1978). https://www.fdic.gov/regulations/laws/rules/6000-1700.html

[8] The Family Educational Rights and Privacy Act of 1974 (FERPA) (20U.S.C. § 1232g; 34 CFR Part 99, enacted August 21, 1974). https://www.law.cornell.edu/uscode/text/20/1232g

a series of reports that explored privacy.[9] [10] [11] [12] And also let's be clear, agencies like to expand their authority, get increased budgets. So FTC really took a claim that it was going to be this privacy enforcer.

And the FTCs initial reports from the late nineties actually said, "We don't need a federal law whatsoever. Instead, the FTC can handle everything by using what's known as its Section 5 authority to police what are deceptive or unfair acts and practices in commerce." And so that's actually what gets you to the creation of the Privacy Policy, because the FTC recommended, "Hey, businesses, you guys should all explain what you're doing with data. And then if you don't do what you say, you don't keep your privacy promises, we can come after you." The state's actually picked up on this, California introduced a law in, I believe 2003, CalOPPA,[13] that required website privacy policies. So that took us down this road of everybody's going to write privacy policies and that's going to be how we keep people accountable. Twenty years later, that clearly has not worked. No one reads these policies. If they do read them, they don't understand them. And the policies also don't get at some of the really thorny ethical issues about what you should or should not do with information.

Bye: I think that history actually helps clarify a lot of things in terms of specifically why Facebook could say that their definition of privacy is essentially that we're just going to tell you what we're recording. So there's a bit of "notice and consent" that seems to have happened with these privacy policies, but that seems to be born out of this FTC mandate,[14] and you traced back through all the history for what that is.

But I know that there's different philosophers of privacy, like Helen Nissenbaum who has contextual integrity,[15] there's Dr. Anita Allen, who is advocating for more of privacy as a human right. And some of her thinking was involved in the creation of GDPR. And then there's others that have a more libertarian take,

[9]FTC Releases Report on Consumers' Online Privacy, June 4, 1998. https://www.ftc.gov/news-events/press-releases/1998/06/ftc-releases-report-consumers-online-privacy

[10]Privacy Online: A Report to Congress, Federal Trade Commission, June 4 1998. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

[11]Site Seeing On The Internet, The Savvy Traveler, Federal Trade Comission (1998). https://web.archive.org/web/20000229073714/http://www.ftc.gov/bcp/conline/pubs/online/sitesee/index.html

[12]About Privacy, Federal Trade Commission (1998). https://web.archive.org/web/19991109041140/http://www.ftc.gov/privacy/index.html

[13]The California Online Privacy Protection Act of 2003 (CalOPPA), (Stats. 2003, Ch. 829, Sec. 3., effective as of July 1, 2004). https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22575.

[14]A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority. Federal Trade Commission. https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

[15]A. Barth, A. Datta, J. C. Mitchell and H. Nissenbaum, Privacy andcontextual integrity: framework and applications, 2006 IEEE Symposium on Security and Privacy (S&P'06), Berkeley/Oakland, CA,2006, pp. 184. Retrieved from https://www.andrew.cmu.edu/user/danupam/bdmn-oakland06.pdf on March 10, 2020.

like Dr. Adam Moore, who, he sees privacy more as like a copyright that you could license out, as an example.[16]

So there seems to be this deeper level of the philosophy of privacy, of what privacy is and what it should mean. And then it gets filtered through this FTC regulation and law that then has a definition of privacy, meaning that we can collect just about anything that we want, and we just have to tell you about it. And if we tell you about it, then it's okay.

Jerome: Right. And I think that the real challenge is, who gets to decide or define privacy really matters here. So Professor Nissenbaum, her theory of contextual integrity is really, really interesting, and everybody's adopted this idea that privacy really depends based on context. And if you're sharing your medical history with the doctor, you understand that, but you don't expect him to share it onward. But what always tends to be missing is that she did follow up writing after that, because her idea was adopted by all sorts of different folks, industry groups liked it, privacy groups liked it, the Obama administration, and it's 2012 Consumer Privacy Bill of Rights[17] [18] used the notion of contextual integrity. And she pointed out that everybody was using that in a slightly different way. And if you define contextual integrity based on whether you're just disclosing information, or if it's in the context of what governments want or what companies want, it subverts her initial aim, which was to get at how society socially constructs our relationships.

So contextual integrity is a really interesting idea that has, I think, unfortunately been warped by all these different proposals that we've seen. And I think the other real tricky challenge – and I don't think I ever answered your question about what I think privacy is – is that we oftentimes conflate – and this is certainly what we're locked into right now with the debate about federal privacy legislation. We have what is known as sort of "Commercial consumer privacy," you know, how are Google and Facebook and a treat your information? What rights did you have to that? And that is entirely divorced from the larger debate about government surveillance, and what does privacy mean under the Fourth Amendment? Now, I think both of those conversations should inform each other, but as a matter of law and active policy, they don't. Again, I'm based in DC, so I'm probably a denizen of the swamp, and pretty frequently you see organizations that are really immersed in consumer privacy. And I don't mean

[16]Privacy Conference: Law, Ethics, and Philosophy of End User Responsibility for Privacy [Video File]. Recorded on April 24, 2015. Retrieved from https://www.youtube.com/watch?v=8WIB_2isRxw on March 10, 2020. University of Pennsylvania Carey Law School, Center for Technology, Innovation and Competition Privacy Conference Website. https://www.law.upenn.edu/institutes/ctic/conferences/privacy/schedule.php

[17]FTC Issues Final Commission Report on Protecting Consumer Privacy.U.S. Federal Trade Commission. March 26, 2012https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

[18]Consumer Privacy Bill of Rights, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy & Promoting Innovation in the Global Digital Economy, February 23, 2012. https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

this to throw anybody under the bus, but Consumer Reports, they're doing really excellent work on what's known as, "The Digital Standard" to try and rate and review products based on how they're protecting privacy, how they're thinking about data security.[19] But Consumer Reports won't touch government surveillance issues with a 10-foot pole.

On the other side of that dynamic, you've got a lot of groups that are really concerned about the government because Google and Facebook and Axiom and Equifax, they can profile us into oblivion, but they can't put us in prison, and so we need to focus on government-controlled information. And so they won't talk about how companies are using information, and that divide really manifests itself in a way that has been really hard to get a good piece of federal privacy legislation moving.

Bye: Well, let's talk about this connection between the government and the companies, because there is a bridge there in what I see at least from the Fourth Amendment being unreasonable searches and seizures, so we should have, especially in enclosed spaces.[20] And there's lots of laws that have come out to say, "Okay, how do you define where we have a reasonable expectation of privacy?" But according to all the cyberspace laws that have come out, all of the cyberspace is essentially a public domain, where with the third-party doctrine,[21] any information you give over to a third party has no reasonable expectation to remain private. So in what Snowden documents have come out, there seems to be a pretty strong link there between information that we give over to these third parties and then the governments with Project Prism and all these other leaks that came out from Edward Snowden. And Snowden has said that the third-party doctrine has been this bridge for how the US government has been able to justify this mass surveillance, which I know that there's been some recent court appeals rulings around that as to whether or not this mass surveillance was legal or not, and actually saying that it wasn't legal. But at the same time, we still have this issue of the third-party doctrine. This interpretation that would require a Supreme Court case and interpretation, the Carpenter Case[22] seems to be an early indication that it's moving towards a world where it's not just a blanket, there is a little bit more contextual dimensions being introduced there. But maybe you could catch us up a little bit on this third-party doctrine and this issue of privacy here?

Jerome: Well, so I think you're right that the Supreme Courts or our judicial

[19]Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace. March 6, 2017. https://www.consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_consumers_security_and_privacy_in_complex_marketplace/

[20]Gilad Yadin, Virtual Reality Surveillance (February 15, 2017). Cardozo Arts & Entertainment Law Journal, Vol. 35, No. 3, 2017, Available at SSRN: https://ssrn.com/abstract=3043922

[21]The Fourth Amendment Third-Party Doctrine. Congressional Research Service (June 5, 2014). https://fas.org/sgp/crs/misc/R43586.pdf

[22]Carpenter v. United States, 585 U.S. _____, No. 16-402. (Argued: November 29, 2017, Decided: June 22, 2018)https://www.oyez.org/cases/2017/16-402

understanding of what constitutes what's protected under the Fourth Amendment is a mess. There's all sorts of scholars from Orin Kerr,[23] [24] to Daniel Solove [25] that have highlighted just the problems with how we think about the Fourth Amendment. And we're seeing this – if you look at the court cases where – the best example of this is US v. Jones,[26] which is a precursor to Carpenter, which was where the Supreme Court held that attaching a GPS device to a car, and then monitoring that device for a long period of time – they don't specify what becomes a long period of time – constitutes a search under the Fourth Amendment. It's a unanimous decision, but there's three different opinions.

Some of the justices are using a property rationale like, "You've attached a physical thing to a car, and the Fourth Amendment is trying to protect our persons, property in our effects." You've got another set of justices that are saying, "Well, there's just too much information going on here, and this offends our notion of a reasonable expectation of privacy." And that emerges out of a Supreme Court case in 1967, the Katz case,[27] which is when the Supreme Court shifted from thinking about privacy, in terms of property, to privacy in terms of reasonable expectations.

And then you have Justice Sotomayor in the middle, who's just acknowledging there's a whole lot of going on here. She appears to embrace what's known as the Mosaic Theory, [28] where when you have all sorts of information coming from different places, it upsets this entire balance.

And so, you don't actually have a decision of what type of vision for privacy that we want in the future.

But I do think that the courts in general – it's not just the Supreme Court – are really waking up to technology. I mean, traditionally, these are old people that have never so much as used an email account. But you look at a case Riley v. California in 2014,[29] when the Supreme Court notes that – usually, when you're arrested, police can search your immediate surroundings to protect themselves, and they were using that as an excuse to say, search cellphones. And you had the Supreme Court acknowledging that cell phones are collecting in one place,

[23]Orin S. Kerr, The Curious History of Fourth Amendment Searches (September 30, 2012). 2012 Supreme Court Review 67 (2013). Available at SSRN:https://ssrn.com/abstract=2154611

[24]Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. Issue 5 (2004). https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1722&context=mlr

[25]Daniel J. Solove, Fourth Amendment Pragmatism, 51 B.C. L. Rev. 1511 (2010),https://lawdigitalcommons.bc.edu/bclr/vol51/iss5/4

[26]United States v. Jones, 565 U.S. 400, (Argued: Nov 08, 2011. Decided: January 23, 2012)https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf

[27]Katz v. United States : 389 US 347. (Argued: October 17, 1967. Decided: December 18, 1967). https://www.oyez.org/cases/1967/35

[28]Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311 (2012). Available at:https://repository.law.umich.edu/mlr/vol111/iss3/1

[29]Riley v. California, 573 U.S. 373, (Argued: April 29, 2014. Decided: June 25, 2014). https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

all sorts of different types of information. And no, searching through contact lists and photos of a phone when you're arresting someone has nothing to do with an officer's safety. So you're seeing this dynamic at work.

And one thing I guess I would push back on you at, is the Supreme Court isn't necessary to overturn the third-party doctrine. Congress can play a role here. Congress can set the standard. One really important piece of legislation that was passed in 1986 is the Electronic Communications Privacy Act.[30] That was a response to the court's understanding of where and when you require a warrant or other types of legal process to intercept electronic communications. The Fourth Amendment is a baseline. Congress can build on top of that, and States have done it. Utah[31] and California[32] have both passed laws that require different types of warrant requirements around information.

And to talk about how this impacts XR, we've seen how it trickles into other types of data areas. A really interesting example of this is in California. Cities like Los Angeles are working on the mobility data specification. [33] They want to create a digital twin – and this has implications for AR – for the transit system. And to do this, they want to collect every bit of information from scooters, but eventually drones, autonomous vehicles, in their city to manage transportation.

And you've got an ongoing lawsuit right now from the Electronic Frontier Foundation and the ACLU of Southern California, saying that this violates California State Law about where and when government can get access to information.[34] We've seen other instances where courts have really – and this is I think, very relevant for virtual reality and augmented reality – courts have under ECPA [Electronic Communications Privacy Act[35], which is a reform of the Stored Communications Act[36]], what's known as a "content versus non-content distinction."[37] So the content of emails can be protected, but the metadata might not

[30]Electronic Communications Privacy Act of 1986 (ECPA), (Pub. L.99-508, 100 Stat. 1848, 18 U.S.C. §§ 2510-2523, enacted on October21, 1986). https://www.congress.gov/bill/99th-congress/house-bill/4952 [More context at: https://epic.org/privacy/ecpa/]

[31]New Utah Privacy Law Expands Warrant Requirement for Individuals' Data Held by Electronic Communications Service Providers. Enacted on March 27, 2019. https://www.jdsupra.com/legalnews/new-utah-privacy-law-expands-warrant-47340/

[32]California Enacts CalECPA, Requiring a Search Warrant to Obtain or Access Users' Electronic Information. Enacted on October 8, 2015. https://www.jdsupra.com/legalnews/california-enacts-calecpa-requiring-a-40462/

[33]Los Angeles Department of Transportation, Mobility Data Specification, October 31, 2018. https://ladot.io/wp-content/uploads/2018/12/What-is-MDS-Cities.pdf

[34]EFF, ACLU File Lawsuit to Stop Los Angeles From Collecting Real-Time Tracking Data on Citizens' Rental Scooters. Electronic Frontier Foundation. June 8, 2020. https://www.eff.org/press/releases/eff-aclu-file-lawsuit-stop-los-angeles-collecting-real-time-gps-tracking-data

[35]Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA). Congressional Research Service. May 19, 2015. https://fas.org/sgp/crs/misc/R44036.pdf

[36]Stored Communications Act (SCA) (Pub.L. 99–508, 100 Stat. 1848,1860, §§ 2701–2712, 18 U.S.C. Chapter 121, enacted on October 21, 1986) https://en.wikipedia.org/wiki/Stored_Communications_Act

[37]Matthew J. Tokson, The Content/Envelope Distinction in Internet Law, 50 Wm. & Mary

be. And under a Sixth Circuit opinion in 2010 US v. Warshak,[38] you really have the court saying, "Obviously content should have extra protections. There's no way Congress intended to let content get into the hands of law enforcement without legal process." And so that applies to the contents of emails, but you could imagine that applying to some of the really deep and detailed information being created in virtual space.

Bye: Yeah, I guess I should give a disclaimer that I am not a lawyer, but I like to play one on my podcast sometimes. So I appreciate the distinctions there.

Jerome: I mean, really, this is me getting on an advocacy, banging my drum. We really do need new legislation. Like this conversation about how we need to have Federal Privacy Law, everybody seems to agree that, yes, we need an update. But we also clearly need updates as to where, when, and how governments can get access to this information. And the sad part is unfortunately, our political system, at least the United States, is so broken right now, despite the fact that we all agree, we can't seem to get anything done. Congress is its own beast. I think what's really important for your listeners to understand is that so much of the debate around federal privacy legislation is going on in the House and Senate Commerce committees,[39] and that's very distinct from the judiciary committees, which basically, those are the committees that pass things like the USA Freedom Act,[40] and other types of surveillance reform around the NSA, in the wake of Edward Snowden. And unfortunately, sometimes committees don't always play nice together and there's turf warfare.

Bye: Yeah, so the one I watched today was the commerce one, I believe. And so there was yeah, things being cast through that economic lens, and not wanting to bring too much regulatory burden. But before we dive into that, I wanted to ask another, I guess, legal question, which is, when I talked to Sarah Downey who has been investing as a VC, but also has a background in privacy law. She said that this reasonable expectation of privacy, in some sense, that's something that is culturally defined.[41] It's a normative standard that evolves over time based upon what people are doing. So as we are giving away more and more of our private data over time, then it seems to me that our reasonable expectation of privacy is perhaps therefore weakened, which would then allow the government to do a lot of those same things that these surveillance capitalism companies have been doing. Do you any comment on how do you determine what a reasonable expectation of privacy is?

L. Rev. 2105 (2009),https://scholarship.law.wm.edu/wmlr/vol50/iss6/5

[38]United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) [Argued:June 16, 2010. Decided: December 14, 2010]http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf

[39]Revisiting the Need for Federal Data Privacy Legislation, Hearing by US Senate Committee on Commerce, Science, and Transportation, September 23, 2020https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation

[40]The USA Freedom Act (H.R. 2048, Pub.L. 114–23, enacted on June 2,2015). https://en.wikipedia.org/wiki/USA_Freedom_Act

[41]Kent Bye & Sarah Downey, "#493: Is Virtual Reality the MostPowerful Surveillance Technology or Last Bastion of Privacy?" Voicesof VR Podast, January 13, 2017. https://voicesofvr.com/is-virtual-reality-the-most-powerful-surveillance-technology-or-last-bastion-of-privacy/

Jerome: No one really knows. I mean, the problem with the original Katz test is it was supposed to have both objective and subjective expectations of privacy.[42] You know, both the individual locked themselves in a phone booth, and that society recognizes that we wouldn't interrupt someone in a phone booth. I think what you're describing is what's been known as the "one-way ratchet," where that test invariably leads to less and less privacy. And I think there's some merit to that, particularly when you have government get into the debate, because they will constantly say that type of argument.

I would push back, and I think actually judges have pushed back pretty strongly, and we're seeing this more and more with cell phones and location data, where the government comes to the court and says, "Well, clearly people know that they're giving this information away. There's no problem here." And the judges, again, maybe because they're old or maybe because they are seeing this the way we're seeing it saying, "No, no, no, wait, wait, wait, wait, wait, wait, wait. Just because – and this gets to a theory of context, just because people are forced by society, we need to have cell phones to function now. And just because people are expecting to give away really sensitive information to doctors or other types of professionals, doesn't mean that they thought that everyone, anywhere, for all time, forever, will get this information.

The Supreme Court in its line of third-party doctrine cases in the 70s and 80s, they clearly keep expanding this doctrine in ways that have privacy advocates, and folks like me wondering, "What are they thinking?" And because they're seeing these things happen one at a time. Oh, police are looking at trash. Police are flying a helicopter over a yard.

But I think it's really important that – there was a case in the late eighties where the Supreme court acknowledges that Dragnet type law enforcement practices, those are going to require courts to establish different constitutional principles.[43] And I think that's what we're seeing now. For a long, long time, all of this super advanced technology was really expensive for law enforcement. There's a really excellent article in the Yale Law Journal from Ashkan Soltani and Kevin Bankston, it tries to basically evaluate the cost of surveillance.[44] And the thing is, surveillance has become so cheap now for law enforcement agencies, that the protections are all out of whack. And I think what you're seeing in all of these Supreme Court cases – but also at the district and circuit court levels – is the courts trying to rebalance what privacy means under the Fourth Amendment.

Bye: There seems to be this tension between trying to mitigate existing harm that's already being done, but also to prevent future harms without unduly

[42]Reasonable Expectation of Privacy Test. Cornell Law School Legal Information Institute's Wex. https://www.law.cornell.edu/wex/expectation_of_privacy

[43]Christopher Slobogin, Government Dragnets, 73 Law and Contemporary Problems 107-143 (Summer 2010). Available at: https://scholarship.law.duke.edu/lcp/vol73/iss3/4

[44]Kevin S. Bankston & Ashkan Soltani, Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones, 123 YaleL.J. Online 335 (2014),http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones

trying to block innovation from smaller players. So there's this tension between wanting to address the harms that are being done, but also to not create some regulatory capture from these major players – that they're the only ones who can afford to even actually follow those rules. And that seemed to be a big part of the discussion of that tension between the small businesses versus the big major tech corps, who have the resources to be able to follow these.

So how does that get resolved when you think about these issues around privacy? And how do you actually negotiate, what seems to be this polar opposite tension between trying to prevent consumer harm, versus not trying to block innovation?

Jerome: Me personally? Or the wider world? Part of it is, we don't thave shared definitions of harms. I do think the notion of a privacy harm has expanded. If you go back in time ten, twenty years, everyone understood that IP theft was a harm, there was a financial harm there. Other types of actual abuses, so for example, where Ashley Madison was the adultery website reveals all this information, that type of embarrassment that was leading people to commit suicide, or get divorced, people finally acknowledged, "Oh, that's a real harm."[45] People obviously understand physical injury is a harm, but we haven't been so good at figuring out what are autonomy harms. What are reputational harms? The types of things that really get at the problems with our digital economy? The idea of we're all being put into filter bubbles and otherwise being manipulated to give up more information, that hasn't been very easily defined or cognizable as a privacy harm.

There've been efforts to expand this. Your listeners might want to look at Intel a couple of years ago, put out this 20,000-word draft privacy proposal that has this page-long definition of different types of harms that we might consider.[46] And I think it'd be useful for folks to start looking at that, and we need to have a conversation – and that's a generic thing to say – about which of those are harms that we actually think we need to legislate around.

As a matter of what would be a good privacy law, the issue with, and I actually do take this point that we don't want to stop innovation, and when you create a privacy law that requires all sorts of risk assessments, and paperwork, and documentation to justify your privacy practices. You do create a scenario where big companies can handle that, and small companies can't.

I'm a privacy advocate and a lawyer, and I certainly don't think we want any startup, their second employee should not be a privacy lawyer. We might want their second employee to think about privacy, but we don't want them to be a lawyer.

So what's the solution to this? You know, I'm echoing some of the past work I

[45]Ashley Madison data breach, July 15, 2015. https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

[46]Intel Drafts Model Legislation to Spur Data Privacy Discussion, November 8, 2018. https://newsroom.intel.com/news/intel-drafts-model-legislation-spur-data-privacy-discussion/#gs.gqeig6.Draft Privacy Proposal:https://usprivacybill.intel.com/legislation/

did while I was at the Center for Democracy and Technology. I think one of the real concerns that we need to address with privacy laws are secondary uses.[47] At today's hearing, there's so much conversation about opt-ins and opt-outs and giving people notices and toggles about things. None of that's ever going to work. It just won't. People don't have the time. It's unmanageable, and there are cognitive limitations and understanding what could happen next. So really you need to find specific practices and types of information you want to sharply curtail.

At the Center for Democracy and Technology, I worked on a draft that would have sharply limited the use of biometric information, sharply limited to use of location information.[48] And the reason for that is because we've seen with facial recognition, it's very hard to put any meaningful controls on the collection of that information.

Similarly, with location, it's been used by stalkers, we've had telcos not actually know how the information they collect is getting in the hands of bounty hunters. So this is information that industry players have either been a little bit mischievous with, or just have not been good custodians of the information. And so I think we probably need laws around that to curtail some of that use.

A lot of privacy advocates are calling for what's known as "data minimization."[49] This idea that, again, you can't use data collected for one purpose for a secondary purpose. And I think this is the issue here – and again, I'm not bothered by shoe ads tracking around the internet, but the underlying technology and the ecosystem that it created, where it creates basically a data free-for-all. And it has created a whole bunch of business models, is highly problematic. We've also created a whole bunch of businesses – and you're a journalist. Journalism, newspapers, media websites, are utterly dependent on online advertising now. So if we were to curtail this through a privacy law, what do we do to those businesses? It's going to be really painful. And we haven't really had that conversation.

Bye: Hmm. Well, after watching the hearing today, one of the other big dynamics that I saw was that you have the GDPR, the General Data Production Regulation, in the European union, that's in some ways shifted the entire culture because all of these big major tech corporations have had to comply with

[47]Ramanathan, T., Schmit, C., Menon, A., & Fox, C. (2015). The role of law in supporting secondary uses of electronic health information. A Journal of the American Society of Law, Medicine & Ethics, 43 Suppl 1 (0 1), 48–51. https://doi.org/10.1111/jlme.12215 Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4687394/

[48]Statement of Joseph Jerome, Policy Counsel, Privacy & Data Project Center for Democracy & Technology before the New York Senate Senate Standing Committee on Consumer Protection New York Senate Standing Committee on Internet and Technology hearing on Online Privacy and Role of Legislature. June 4, 2019https://cdt.org/wp-content/uploads/2019/06/2019-06-03-NY-State-Joe-Jerome-Testimony.pdf

[49]Principle of Data minimisation. United Kingdom Information Commissioner Office's Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

that. So they've had to change their underlying technological architectures.

Then you have individual states within the United States, with California having with their data protection. You have Washington state that trying to pass one, it didn't pass. You have Illinois with the biometric law. So you have these different states that are innovating when it comes to privacy, and you have this tension with this discussion, talking about this federal privacy as to whether or not this federal law is going to preempt all these regional laws. Whether it's going to be a baseline floor that you can build on top of. Or if it's trying to set a privacy ceiling so that those states could not go beyond that.

So there seems to be this dialectic between both the GDPR and having the United States come up with something that is equivalent. And there's a fragmentation within all these different federal laws already at this point, where it's not like a one-stop shop where you can go and see what the privacy laws in the US are. It's really all over the place and already super confusing. So yeah, on top of that, adding all the individual states that are having their own.

So how do you make sense of some of the biggest hot topic debates of preemption, the floor versus the ceiling, and you know what's happening?

Jerome: You should need to interrupt me if I get too wonky, because preemption is a very technical and weedy topic. I think you accurately described the situation where we, in some respects, want states to be laboratories of democracy. On the other hand, the internet is global and having internet rules for, as it was described in the hearing today, Mississippi and Washington state don't make a whole lot of sense.

I think adding a wrinkle to that with, just to talk a little bit about mixed reality, you have the fact that facial recognition is a perfect example of this. We might want one national standard for how facial recognition is deployed when it's being used in a Facebook photo tagging sense. But that maybe doesn't work in the context of facial recognition at storefronts at brick and mortar stores, because shouldn't we want the right of a community to say, "We don't want this technology." As mixed reality infects or it crosses with the real world, states and localities are really good at passing laws to deal with safety and their local concerns.

But now they're being asked to govern technology. So that's a really tough dynamic that the preemption debate hasn't really thought of because you're looking at these different federal proposals and some of them would preempt all sorts of state laws, including the earlier state laws I was talking about with respect to government access to information. Because if we want to preempt all privacy laws, do we want to preempt government laws that impact privacy? They might arguably preempt – I work at Common Sense, we do a lot of work on student information. So you think about VR headsets in the classroom. What does that mean? Well, our federal student privacy law is from the 1970s. States have been passing state-based privacy laws over the past five years. They're much newer they're much more adapted to a universe where kids' permanent

records aren't in file cabinets, they're in the cloud. But would your federal law preempt that?

I think AR and VR have tremendous applications in employment. Employment law tends to be something that's very much regulated at the state level. Would your federal law preempt that? These are really, really tough questions. I actually think – just to say what the general philosophy of what preemption should be.

I think preemption is a question that a federal proposal has to address last. There've been good reports from professor Peter Swire who helped with the health privacy rule and the Brookings Institute that tried to explore the really tough legal complications of preemption.[50] [51] And really you can't decide what state laws you want to preempt until you've written the entire rest of the law, because there's hundreds of state laws that could be impacted.

I think about VR and AR present interesting health questions, but you have state laws that govern say disclosures and controls around HIV status. Well, maybe you want to have a national standard for that, but you can't make that decision until you've seen the complete law. So, preemption is, again, it's something you really have to do at the end.

I think you also – and this always comes up – the federal government is not good at updating laws. With technology, you can't just pass a law once and never get back to it. I mean, the law will become out of date pretty quickly and we give the GDPR[52] a lot of credit, but the GDPR was a replacement for the 1996 Data Protection Directive.[53] That was twenty years later, they updated their framework. Are we going to put in place some mechanism to update our framework over time? One idea that we initially had at CDT a long time ago, was that you pass a federal law, but parts of it could sunset over time.

That means it would stop being enforced. I mean, this would, again, after three, five, eight years in the future, if we found that there were gaps in protection, states could then step into the breach. I think you need to explore that type of stuff. You also need to explore – and I don't think we've done a good enough

[50]Peter Swire, "US federal privacy preemption part 1: History of federal preemption of stricter state laws" International Association of Privacy Professionals, January 9, 2019https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/

[51]Peter Swire, "US federal privacy preemption part 2: Examining preemption proposals" International Association of Privacy Professionals, January 10, 2019https://iapp.org/news/a/us-federal-privacy-preemption-part-2-examining-preemption-proposals/

[52]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General DataProtection Regulation)https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[53]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to theprocessing of personal data and on the free movement of such data https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

job of this – how would this new federal privacy law not just intersect with state law, but the other federal privacy laws? We've got health privacy laws. We have a really crappy financial privacy law. Are we going to update those? And if we don't update them, that seems like a missed opportunity too.

Bye: At today's hearing, there was Julie Brill, a former FTC commissioner, now she's the Chief Privacy Officer at Microsoft. And she said there's been more privacy laws in the last nine months then there have been in the last thirty years, in terms of legislation being suggested.[54] So it seems like it's a hot topic right now –

Jerome: Yes. It is keeping me employed.

Bye: But what I noticed was the ones that have been submitted, there's ones that are created by say all Democrats, and then another one by all Republicans. And so there doesn't seem to be a across-the-aisle, multi-party perspective. It's very partisan perspectives. And I think this speaks to some of your skepticism as to how this is going to play out, because there seems to be a polarization between how this actually gets implemented in – for example – if a private right to action could be Democrats advocating for it and Republicans not.

How do you navigate this landscape as to everybody wants this, but the political polarization seems to have been replicated within even this privacy issue – where you have people that are so entrenched into their own issues?

Jerome: Yeah. And I think that's unfortunate. I mean, my favorite privacy bill is actually the House Energy and Commerce Committee discussion draft, which, because they couldn't resolve certain stuff, just bracketed certain sections entirely.[55] It'll either have a private right of action or it won't. It'll either apply to small businesses or it won't. So, you're right.

My general default nature is Mr. Doom and Gloom. I think there is something to be said that the privacy proposals we're seeing, do have quite a bit of overlap.[56]

[54]Written Testimony of Julie Brill Before the United States Senate Committee on Commerce, Science, & Transportation Revisiting the Need for Federal Data Privacy Legislation, September 23, 2020. https://www.commerce.senate.gov/services/files/5404DCED-136B-4622-B922-49045EC7C03E [

[55]James Yoon, "House Energy and Commerce Committee Circulates Draft Privacy Bill Expanding FTC Authority" December 19, 2019https://www.insideprivacy.com/united-states/congress/house-energy-and-commerce-committee-circulates-draft-privacy-bill-expanding-ftc-authority/[House Energy and Commerce Committee draft bill, December 18, 2019:https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/2019.12.18-Privacy-Bipartsian-Staff-Discussion-Draft.pdf]

[56]Cantwell, Senate Democrats Unveil Strong Online Privacy Rights New consumer rights guaranteed by strong federal compliance and consumer right to sue. Data companies with security breaches can be fined.November 26, 2019. https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights

57 58 59 60 61

You're right that we don't agree on things like preemption and private rights of action. And I think the problem with that is on all sides, I think privacy advocates have dug in their heels and are asking for too much, but I don't want to throw my friends and allies under the bus. I think most of the blame comes from industry groups, particularly trade associations.

They refuse to see the writing on the wall here. I remember I was talking to a couple of trade associations that, they all absolutely hate the California Consumer Privacy Act.[62] They all absolutely think we need a federal privacy law. And my question to them was, "Well, do you like anything in the CCPA? Because you can't just say, 'We're going to get rid of this and start over' without giving that initiative some credit." *[Note: here are some other state privacy law initiatives from California* [63] [64] *and Washington* [65] [66] [67]*]*

Plus you have to realize as a political reality, California is a huge state, huge part of the congressional delegation. The Speaker of the House is from California. So you're just saying that her home state's law is terrible and you have no actual alternative. That's not going to fly.

---

[57]Cantwell (D-WA), Schatz (D-HI), Klobuchar (D-MN), & Markey(D-MA), S. 2968, the "Consumer Online Privacy Rights Act" (COPRA), November 26, 2019 https://www.congress.gov/bill/116th-congress/senate-bill/2968/text

[58]Sen. Moran Introduces Landmark Federal Data Privacy Legislation, March 12, 2020. https://www.moran.senate.gov/public/index.cfm/news-releases?ID=5C11EECE-DE43-4B2B-AEDE-76504D1D6186

[59]Moran (R-KA), S. 3456, the "Consumer Data Privacy and Security Act of 2020," March 12, 2020. https://www.congress.gov/bill/116th-congress/senate-bill/3456/text

[60]"Wicker, Thune, Fischer, Blackburn Introduce Consumer Data Privacy Legislation", September 17, 2020. https://www.commerce.senate.gov/2020/9/wicker-thune-fischer-blackburn-introduce-consumer-data-privacy-legislation

[61]Wicker (R-MS), Thune, (R-SD), Fischer, R-NE, Blackburn, (R-TN), "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" (SAFE DATA Act), Sep 17, 2020. https://www.commerce.senate.gov/services/files/BD190421-F67C-4E37-A25E-5D522B1053C7

[62]The California Consumer Privacy Act of 2018 (CCPA) [1798.100 -1798.199], Enacted on June 28, 2018. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[63]California Proposition 24, Consumer Personal Information Law and Agency Initiative. Ballotpedia. (2020)https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020)

[64]Californians for Consumer Privacy, The California Privacy Rights Act of 2020 - Ballot Initiative. September 2019https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020-ballot-initiative/

[65]FPF Staff. "A New U.S. Model for Privacy? Comparing the Washington Privacy Act to GDPR, CCPA, and More" Future of Privacy Forum. February 12, 2020https://fpf.org/2020/02/12/a-new-model-for-privacy-in-a-new-era-evaluating-the-washington-privacy-act/

[66]Khari Johnson, "Washington Privacy Act fails again, but state legislature passes facial recognition regulation" Venture Beat March 12, 2020https://venturebeat.com/2020/03/12/washington-privacy-act-fails-in-state-legislature-again/

[67]Washington Senator Reuven Carlyle. Washington Privacy Act 2021 (WPA)[Draft]. August 5, 2020. https://sdc.wastateleg.org/carlyle/wp-content/uploads/sites/30/2020/09/WPA-2021-DRAFT-Carlyle.pdf

I've written about this a couple of times, both for the International Association of Privacy Professionals [68] and also for a symposium that Tech Dirt blog[69] did about thorny issues and privacy. And I was saying, "We really got to throw some other ideas out there about…" My bugaboo has been about enforcement. How is the law going to be enforced?

But similarly with preemption, there are lots of people out there thinking about these areas of the law that are not privacy and technology policy wonks.[70] These are people that have been working in civil rights laws. These are people that have worked at the intersection of state and federal law, Federalism 101, that should be weighing in and we should go seek their advice. And we haven't really done that.

I think there is room for compromise. We should stop saying the word "private right of action," which is this ability to go sue a person in court. I think we need to be talking about redress. How are we going to solve problems when they occur or when we see them. And you can come with a whole lot of other different solutions to that, that go beyond just people bringing lawsuits. I've offered up a couple of them.[71] You either narrowly tailor the lawsuit. So one example – there are problems with all of these – but realistically, what happens now is one person has an issue. They find a plaintiff's firm to try and bring a lawsuit and they bring a class action and they get a bunch of money at the end of the day. That is what's happened with a lot of the litigation around Illinois' Biometric Law,[72] it just is what happens often.

An alternative model I'd throw out there is, can that person work with a public interest organization, the EFFs of the world, the ACLUs of the world, to bring a lawsuit that would do injunctive relief as opposed to monetary relief? Is that something companies would be open to? They don't say anything except the tagline you'll get from almost all companies is, "We believe in strong enforcement and that should be led by the FTC and state AGs." Okay. I mean, I think we need to break it up and say a little bit more than that.

---

[68] Joseph Jerome. "Can FTC consent orders effectively police privacy?"International Association of Privacy Professionals. November 27, 2018. https://iapp.org/news/a/can-ftc-consent-orders-police-privacy/

[69] Joseph Jerome. "Can You Protect Privacy If There's No Real Enforcement Mechanism?" Tech Dirt, May 29, 2020. https://www.techdirt.com/articles/20200529/11155744607/can-you-protect-privacy-if-theres-no-real-enforcement-mechanism.shtml

[70] Cameron F. Kerry, John B. Morris, Jr., Caitlin Chin, and Nicol Turner Lee. "Bridging the gaps: A path forward to federal privacy legislation," Brookings Institution, June 3, 2020https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/

[71] Joseph Jerome. "Private right of action shouldn't be a yes-no proposition in federal US privacy legislation." International Association of Privacy Professionals. October 3, 2019 https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/

[72] Jeff John Roberts, "Facebook users in Illinois can now apply for aprivacy payout of up to $400" Fortune, September 22, 2020. https://fortune.com/2020/09/22/facebook-privacy-payouts-illinois-fb-pictures-tagged-photos/

Bye: Yeah. So the private right to action – in the hearing today, they talked about the private right to action. And when I looked into it a little bit and actually read your article, it seems to be the issue is that there is one police force, which is the Federal Trade Commission, which has the remit to enforce these different privacy laws. But you also mentioned the state attorney generals and that we shouldn't just rely upon just them as the only enforcer, but that if there's harm that's done, then there should be the ability for people to have either class action lawsuits or to have individual lawsuits that were trying to represent the harms that are done, that maybe go above and beyond what the FTC is able to have the time and energy to enforce. Is that the essence?

Jerome: Yes. I mean, that's why I'm saying we need other mechanisms to act as police. I mean, another idea that I've thought about – and this is a half-baked idea is – how do we find information to qualified independent researchers? So this is something we've seen happen quite a bit with Facebook.

A lot of the action against Facebook against discriminatory housing ads or employment ads. These are investigations that are being done by ProPublica[73] and the Markup[74] and other journalistic outlets. These companies are sitting on huge amounts of data. If we can inject third-party researchers to understand how these algorithms are being developed, maybe that is another way to solve some of these issues.

There's other interesting ideas – and this was initially noodled by Professor Ryan Calo and came up in the Obama administration's privacy efforts – was the idea of a privacy review board.[75] [76] Could you create some quasi-independent board within companies, outside of companies, that would approve or monitor corporate data practices and would then give them a thumbs up, thumbs down, could report those practices to the FTC, could make those practices public? That doesn't solve all the issues, because you have to figure out how to make that entity sufficiently independent.

But you're already seeing efforts like that in related areas. Facebook is setting up the oversight board,[77] which is this weird, extra-judicial, global body

[73] Julia Angwin & Terry Parris Jr. "Facebook Lets Advertisers Exclude Users by Race" ProPublica, October 28, 2016. https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

[74] Jeremy B. Merrill, "Does Facebook Still Sell Discriminatory Ads?" The Markup, August 25, 2020 https://themarkup.org/ask-the-markup/2020/08/25/does-facebook-still-sell-discriminatory-ads

[75] Ryan Calo, Consumer Subject Review Boards: A Thought Experiment (September 3, 2013). 66 Stanford Law Review Online 97-102 (2013), Available at SSRN:https://ssrn.com/abstract=2340745

[76] Kent Bye, Adam Gazzalley, Walter Greenleaf, & Susan Persky, "#716:VR Privacy Summit: Medical Insights into VR Privacy + Health Benefits of Biometric Data" Voices of VR Podcast, November 22, 2018. https://voicesofvr.com/716-vr-privacy-summit-medical-insights-into-vr-privacy-health-benefits-of-biometric-data/

[77] Mark Zuckerberg. "A Blueprint for Content Governance and Enforcement" Facebook. November 15, 2018. https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/?hc_location=ufi

that's going to deal with content moderation decisions on Facebook and they're bringing together judges from across civil society and the globe. [78]

You can envision ideas like that in the virtual space. I mean, that's obviously pretty far removed from congressional legislation, but you already see a little bit about that in some of these efforts where the DETOUR Act introduced by Senator Warner and Fisher,[79] [80] which is incorporated in one of the Senate privacy proposals up for debate, calls for the Federal Trade Commission to create these standards bodies that could observe how companies are ruling out dark patterns.

None of that is going to necessarily make diehard privacy fanatics and advocates happy. But I think those are creative solutions that we ought to be exploring through a legislative process.

And I frankly wish companies would be just more vocal about what they think would be necessary. And I think the problem is, it can't just be Facebook. Facebook says it wants to be regulated, and nobody really trusts them on that. But there's a host of other companies out there that are either better on privacy or better on data that are pretty silent as to what they think would be a good proposal.

Bye: Hmm. I wanted to dive in into the AR and VR specific stuff here in a bit, but I wanted to just kind of wrap up the big, global context before diving into the XR specific things. Because just in the news yesterday in Vice,[81] they were talking about Ireland had a Data Protection Commission that was basically bringing about what seems to be a result of the Schrems II decision[82] the EU that was invalidating this EU to US privacy shield.[83] And so now people that live in the European Union could potentially have Facebook have to meet all these different obligations to not share user data. And Facebook was threatening to potentially pull out of the entire European Union yesterday. I don't know if that was hyperbole or if it was just an idle threat or what that actually means.

[78] Nick Clegg, "Welcoming the Oversight Board" Facebook, May 6, 2020. https://about.fb.com/news/2020/05/welcoming-the-oversight-board/

[79] "Senators Introduce Bipartisan Legislation to Ban Manipulative 'Dark Patterns'" April 9, 2019. https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns

[80] Mark R. Warner (D-VA) and Deb Fischer (R-NE), S.1084 - Deceptive Experiences To Online Users Reduction (DETOUR) Act, April 9, 2019. https://www.congress.gov/bill/116th-congress/senate-bill/1084/text

[81] David Gilbert, "Facebook Says it Will Stop Operating in Europe If Regulators Don't Back Down" Vice. September 21, 2020https://www.vice.com/en/article/889pk3/facebook-threatens-to-pull-out-of-europe-if-it-doesnt-get-its-way

[82] Caitlin Fennessy, "The 'Schrems II' decision: EU-US data transfers in question" International Association of Privacy Professionals. July 16, 2020. https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/

[83] Joshua P. Meltzer, "The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security" VoxEU. August 5, 2020https://voxeu.org/article/impact-gdpr-data-flows-and-national-security

But there seems to be even in the United States with TikToK,[84] having to say, "President Trump trying to ban TikTok and say, 'Okay, how is this data being treated?' " I mean the same type of thing. It's the Communist party of China is involved in aggregating data on the United States citizens, then President Trump has certainly sees that as a threat to try to stop that. And it's reasonable to think of this as a trend of where things are going, that other countries might say the same thing about US companies having the transfer of private data of their citizens being transferred over to the United States, and potentially get into the hands of the US government. So what's going on with Max Schrems, and this whole dynamic here?

Jerome: Max Schrems is the perfect example of how a single privacy advocate properly empowered under the GDPR can cause a whole lot of headaches and ruckus for major companies, not just Facebook, but also data brokers. [85] So I think it's important to acknowledge that A, you've highlighted it perfectly. Schrems is not really about Facebook's data practices. It's about US surveillance practices,[86] [87] [88] which is something also, as I said up top, is something we need to reform and unfortunately isn't generally part of the consumer privacy conversation.

To be perfectly honest, I think both scenarios where Europeans routinely – let's be honest, they go after American companies. The French CNIL [Commission Nationale del'Informatique et des Libertés], for example, has been very aggressive against American companies,[89] [90] [91] but it hasn't gone after Ubisoft, which is a French video game company. My understanding is that they are perfectly kosher with everything Ubisoft's doing. There are a couple of French data bro-

[84]Tali Arbel, Matt O'Brien, & Matt Ott. "US bans WeChat, TikTok from app stores, threatens shutdowns" Associated Press. September 18, 2020. https://apnews.com/article/national-security-china-archive-united-states-a439ead01b75fc958c722daf40f9307c

[85]Hannah Kuchler, "Max Schrems: the man who took on Facebook – and won." Financial Times. April 4 2018. https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544

[86]Andrew Serwin, "White Paper – An Overview of US Surveillance in Light of 'Schrems II' " International Association of Privacy Professionals. August 7, 2020. https://iapp.org/resources/article/overview-us-surveillance-light-of-schremsii/

[87]"Privacy in the EU and US: A debate between Max Schrems and Peter Swire." Brussels Privacy Hub Event at Computers, Privacy and Data Protection Conference. January 26, 2016 [Posted to YouTube Feb 11,2016] https://www.youtube.com/watch?v=dyH7uP_QxGY

[88]Peter Swire, The System of Foreign Intelligence Surveillance Law (2004). 72 George Washington Law Review 1306 (2004), Ohio State Public Law Working Paper No. 18, Georgia Tech Scheller College of Business Research Paper No. 2015-18, Available at SSRN:https://ssrn.com/abstract=586616

[89]Alan Toner, "French Data Protection Authority Takes on Google" Electronic Frontier Foundation. February 13, 2019. https://www.eff.org/deeplinks/2019/02/french-data-protection-authority-takes-google

[90]"The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC" Commission Nationale del'Informatique et des Libertés (CNIL). January 21, 2019 https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[91]Reuters Staff. "Facebook fined 150,000 euros by French data watchdog" Reuters. May 16, 2017. https://www.reuters.com/article/us-facebook-france/facebook-fined-150000-euros-by-french-data-watchdog-idUSKCN18C10C

kers – I'm drawing a blank on their names – that they haven't gone after.

So there is some of this going after the other country. And I think that's exactly what we're seeing, what the TikToK example, where I think the Trump administration has seized on some legitimate concerns and legitimate problems and is extorting companies to act the way the country wants.

And I think we face a very real challenge where we're going to have – I guess the phrase is the balkanization of the internet,[92] separate internets are going to appear, there'll be an EU internet. There already is a Chinese internet. We're on this race as it looks like we're going to have a US internet, that's going to be much, much smaller.

And historically the United States was at the vanguard of pushing for Internet freedom and a broad global Internet. And I think our failure of leadership, both in terms of what we're seeing with extorting TikToK, but also frankly, not adapting to privacy regulations, generally being fairly obstinate on trying to put in place regulations online, has made it so we've seeded global leadership to other countries that we might not want.

Bye: Yeah. And I guess it's interesting to look at TikTok in the context of what is already happening with US companies, because there seems to be – if we did have a federal law that all of the US companies were following, and that we were expecting foreign companies to follow, then you'd have less of this singling out TikToK, just because it's happens to be owned by China. But also what about the US companies that are potentially doing the exact same thing?

Jerome: Right? Yeah, no, and I think that's exactly on point. Another thing that I thinks worth mentioning in the XR context is, again, let's be clear, European regulators want to aggressively police technologies. They see that as their value add, and they want to go after American companies and Facebook has been target number one. We've seen in Germany, for example, their federal cartel office, which deals with their competition laws, try to use the GDPR to unbundle permissions between Facebook, Instagram, and WhatsApp,[93] which I think is having implications for Oculus right now.[94]

So we have a mess of – And I think the United States is behind the eight ball here, but even globally, we have just a confused mess of not just data privacy – and I don't think we want to even say privacy data protection writ large, with competition rules and content moderation and intellectual property. And it's

[92]Mark A. Lemley, The Splinternet (July 30, 2020). Stanford Law and Economics Olin Working Paper #555, Available at SSRN:https://ssrn.com/abstract=3664027 orhttp://dx.doi.org/10.2139/ssrn.3664027

[93]Natasha Lomas. "Facebook succeeds in blocking German FCO's privacy-minded order against combining user data" Tech Crunch. August 26, 2019 https://techcrunch.com/2019/08/26/facebook-succeeds-in-blocking-german-fcos-privacy-minded-order-against-combining-user-data/

[94]Kyle Orland. "Facebook halts Oculus Quest sales in Germany amid privacy concerns" Ars Technica. September 3, 2020. https://arstechnica.com/gaming/2020/09/facebook-halts-oculus-quest-sales-in-germany-amid-privacy-concerns/

creating this giant mess of, who knows what rules should or could apply across borders.

Bye: Yeah. Maybe you could elaborate on this coupling because the data coupling restrictions and GDPR in Germany at least, the Oculus had to be revoked from being sold. I think even people in Germany are not able to pre-order the Oculus Quest 2, because there's this coupling prevention within GDPR to have say one thing connected and coupled to another thing in this case, the requirement of a Facebook account coupled to the ownership of a piece of hardware. So maybe you could expand on this coupling and what you expect to happen there.

Jerome: So the lawyer disclaimer, no one should ever claim that they are an expert on the GDPR. And I certainly won't claim to be an expert on German competition law. But I think what you're seeing here is a really creative interpretation of the GDPR. The GDPR was designed to be enforced by data protection agencies, and now we have a competition authority getting involved. And I think that's because in the EU, they have a much broader understanding of what a competitive harm could be here. And they want to leverage laws across different expertise. As a practical matter, let's be clear, under the GDPR, you're supposed to be – I should have at this point memorized the laundry list of adjectives that go along with what constitutes consent under the general data protection regulation, but it's supposed to be informed. It's supposed to be granular. It's supposed to be specific.[95]

And as a result, the click it wants – and you agree to everything approach that we have developed in the United States is not kosher in the European Union. That doesn't mean that there aren't plenty of companies still doing that and creating "I agree" boxes that you can't really disagree with. But Europe, I think to their credit, has said, "If we're going to have this consent framework, consent should be in some respects meaningful. And you should be able to withdraw consent." And that flies in the face of – I think to be fair, I think Facebook has some legitimate interests in trying to blur all of these accounts and bring everything under one umbrella, but it creates real issues for them.

And I don't want to be such a giant GDPR booster because I think there are problems with that framework, but a lot of people have said, "Well, what has it really changed?" Well, this is what changes. It's taken a few years for enforcers to get up to speed. But if you want to enforce the letter of the law over there, it's going to be unclear to be honest, how some companies can do the stuff that they want to do under the GDPR. Fortunately I'm not a European data protection expert or a compliance lawyer that has to figure it out. But, I think there are plenty of sleepless nights at Facebook trying to handle EU law.

Bye: Yeah. It's certainly entering into a new phase and I appreciate the backstory and context there because I think it's for not only Facebook for anybody

[95] "What are the GDPR consent requirements?" General Data Protection Regulation (GDPR) Websitehttps://gdpr.eu/gdpr-consent-requirements/

who's going to be working in this industry will have to be to some degree, up to speed to some of this stuff. But let's maybe move on to some of the XR-specific things. I know that you've been interested in VR for a while and you've actually done some writing on this topic.[96] And so maybe you could just talk a bit about what is different and new from your perspective when it comes to mixed reality, extended reality, virtual and augmented reality, all the realities when it comes to privacy concerns.

Jerome: I don't know if I'll have good answers compared to some of your expert guests, because I guess with XR, I almost want to say everything and nothing for some of this stuff. Look, if I was looking at XR from a purely privacy compliance standpoint – let's look at the CCPA, I would look at headsets and the types of data collection that's being absorbed by primarily headsets, but also apps that aren't using AR. And I would go through the laundry list of stuff that the CCPA requires. If it has an access request, all right, I'm supposed to give people access to all of the specific pieces of personal information they provide. Okay, well, so companies almost always interpret that to me, and you can give them a list of purchases. We'll give you your email address, something like that.

But in an XR context, what type of logging information, what type of technical information do we want to actually provide people? And even if we're legally required to provide that type of information, what use is it going to be? And I think that's another real challenge here. A lot of our traditional privacy rights, access, correction, deletion, what good is that really going to be in XR?

Deletion always presents really tough challenges. I think deletion will be very, very difficult when it's one thing to delete a person's profile in XR, but what is that going to mean when you have an AR, an annotated universe? I always use the example of the digital "kick me" sign in AR. At least in the United States, we have the public square where people are able to put up signs, protest, assemble. Presumably some amount of public information can be attached to people.

What rights are we going to have to delete that information, particularly if it's true? And this is maybe a grim example, but being branded as a sex offender. In AR, it's just another way to designate that someone's a sex offenders as they're walking around the world. Well, where and when do we think that that type of annotation should be deleted? That's a good question. We've seen new discussions, the Federal Trade Commission, speaking about them again, held a workshop just yesterday on data portability.[97]

I think data portability in XR is really interesting. I know you've been con-

[96] Joseph Jerome. "Establishing privacy controls for virtual reality and immersive technology." International Association of Privacy Professionals. September 9, 2020. https://iapp.org/news/a/establishing-privacy-controls-for-virtual-reality-and-immersive-technology/

[97] Data To Go: An FTC Workshop on Data Portability. September 22, 2020 https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability

cerned and some of your guests have been very concerned about the closed ecosystem that Facebook is creating with Oculus. Well, does data portability let us escape that? I don't know. We might want to explore that, because there have been organizations, like New America's Open Technology Institute, was really interested in exploring whether we could make the social graph that Facebook has, properly exportable, so you could have competing services.[98]

Well, what about VR or AR should be properly exportable? I tend to think that long-term, if we have a static and consistent persistent digital avatar. Or frankly, we've mapped our private homes, should that information be easily portable as a profile to another service? Probably. That seems like something that we might want to explore. But that hasn't been part of the existing privacy conversation in a way that, to my appreciation, I get.

One final thing is, what gets really tough about privacy law, is that it creates a universe of information that is protected and is not protected. And that protected information is personal data, however we want to define it. Whatever is not personal data, we don't care about. I think XR really reveals that that framing doesn't work very well anymore. There is a notion of collective privacy that I think we need to embrace.

We've seen examples of Strava, which is the fitness social network, was revealing military bases because this was aggregated information and it was otherwise reveal it, even if you people were selecting physical spaces that were not going to be mapped, you could reverse engineer that information to figure out private spaces.[99] Well, I think that company looked at this as not really a privacy issue, but maybe just a data management issue, but I think collective privacy and XR really will matter.

So in one of the pieces I wrote about, I was calling for more disclosures around mapping.[100] I think mapping is particularly important. I know you've focused on things like eye tracking,[101] and all the types of biometric information collected from these devices. Now, we have biometric privacy laws, but those laws are again, more focused on things like facial recognition.

With XR, you're going to have – what are the expressions? Diane Hosfelt

[98] Eric Null & Ross Schulman, "The Data Portability Act: More User Control, More Competition" New America Open Technology Institute. August 19, 2019 https://www.newamerica.org/oti/blog/data-portability-act-more-user-control-more-competition/

[99] Alex Hern. "Fitness tracking app Strava gives away location of secret US army bases" The Guardian. January 28, 2018. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

[100] Joseph Jerome. "The Race to Map Reality so Silicon Valley Can Augment It Is On" Slate, September 18, 2020. https://slate.com/technology/2020/09/facebook-augmented-reality-project-aria-mapping.html

[101] Kent Bye & Jim Preston "#516: Privacy in VR is Complicated & It'll Take the Entire VR Community to Figure it Out" Voices of VR Podcast, March 17, 2017. https://voicesofvr.com/516-privacy-in-vr-is-complicated-itll-take-the-entire-vr-community-to-figure-it-out/

describes it as "biometrically deferred information"[102] [103] and Britain Heller wrote a report for this, it's called "Biometric Psychography."[104] That's all information that isn't really properly governed by, I mean, we have antiquated privacy laws here already, but isn't really necessarily properly governed by the GDPR, which is very much focused on individuals and not collectives. And it's not focused on this isn't a privacy issue, but so much as the larger ethics of whether we should or should not be doing this type of processing of data writ large.

Bye: Yeah, I guess my concern is specifically around the differentiation at this point for what is referred to as the Personal Identifiabl Information (PII)[105] [106] [107] [108] versus the de-identified and anonymized data in some ways. And I guess from looking at what the researchers have been able to find is that, what we think is de-identified data, actually, usually isn't. It's usually able to be identified with some level of biometric marker.

Jerome: That's completely accurate. I've done a little bit of work on de-identification, and how we probably don't want to exempt de-identified data from law entirely. But my gentle pushback – and there are organizations that have done a lot of work, the Future of Privacy Forum, for example, has this spectrum of identifiability where there's different levels of identifiable information.[109] My gentle pushback is researchers and academics actually make a career, Latanya Sweeney has made a career out of re-identifying medical records in very specific situations.[110]

But again, is the information made available publicly? I guess my response is, there is no way to 100% guarantee mathematically, that information will be anonymous. It's not possible. So what degree of certainty are we willing to live with or accept or permit companies to still do things with? 90%? 99%? 99.9%? I think we need to ask ourselves that and also realize that it shouldn't

[102]Diane Hosfelt, "Making ethical decisions for the immersive web" arXiv.org, May 14, 2019. https://arxiv.org/abs/1905.06995

[103]Diane Hosfelt, "Making ethical decisions for the immersive web" Mozilla May 15, 2019. https://blog.mozvr.com/making-ethical-decisions/

[104]Brittan Heller. "Reimagining Reality: Human Rights and Immersive Technology." Carr Center Discussion Paper Series, 2020-008. June 12, 2020. https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf

[105]Lucas Long. "PII, Personal Data, and Personal Information: What's So "Personal" About It, Anyway?" Info Trust. March 4, 2020. https://infotrust.com/articles/pii-personal-data-personal-information-whats-so-personal-about-it-anyway/

[106]"GDPR Personal Data." General Data Protection Regulation (GDPR) Website https://gdpr-info.eu/issues/personal-data/

[107]"Guidance on the Protection of Personal Identifiable Information" United States Department of Labor Website. https://www.dol.gov/general/ppii

[108]Kelsey Finch, "A Visual Guide to Practical Data De-Identification" Future of Privacy Forum, April 25, 2016. https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/

[109]Lydia de la Torre, "What is "personal information" under CCPA?"California Lawyers Association. https://calawyers.org/antitrust-ucl-and-privacy/what-is-personal-information-under-the-california-consumer-privacy-act/

[110]Curriculum Vitae of Latanya Arvette Sweeney, Ph.D. http://latanyasweeney.org/cv.html

be necessarily be an all or nothing situation.

The computer scientists and academics and researchers are incentivized to try and prove the information is not sufficiently de-identified. That doesn't mean it's easy for everyone, or even a company that is acting within the law, to re-identify information.

And I think that's actually something we need to recognize. Where a lot of these hypotheses, or hypos are assuming the worst possible actors. And there's always going to be bad actors in these spaces, particularly with XR. I mean, you just think of the laundry list of negative applications in your [XR] ethical manifesto,[111] there's going to be companies that ignore that, entirely. So if we have laws in place to go after those guys, while trying to constrain or incentivize other companies to do other things around de-identified data, that might be good enough.

I mean, I come back to basic security protocols. There are controls you can put in place around this information. I mean, obviously you've got the tech companies leading the way with really advanced analysis of information, but also basic security protocols and administrative controls.

We talk a lot about how advanced companies need to be when they're de-identifying data, and obviously I think that there's a lot of room there to do more research, and understanding about what it means to de-identify eye-tracking technology. I don't have the answer to that. But I also think at a basic level, you got a lot of companies out there that still just don't use basic security technologies. They don't encrypt stuff. They don't throw away data they don't need. And we might actually just want to incentivize basic security practices before we get too obsessed about how impossible it is to de-identify XR data.

Bye: Yeah. I guess two of the risks that I see in where the practices of these companies to hoard as much data as they possibly can, even if they don't know what they're going to do with it. They're going to be gathering this data, perhaps to psychographically profile us. But also perhaps to just train AI on it, and to be able to do things they wouldn't be able to do otherwise. I think the way in which the privacy policies are written, it doesn't limit the context or the bounds of how much of this data they can –

Jerome: Oh, no, no. Not at all. No, no, no. I mean, look. Privacy policies do not protect individuals. They are designed as liability shields for companies. I have written privacy policies for companies. You want to have maximum flexibility. Even if you're a company, and I've heard this with clients, "Oh, we want to be good on privacy." I'm always like, "Well, are you going to not do any types of advertising? Because as we discussed, online advertising enters an ecosystem that's out of control." "Well, no. How are we going to make money?"

[111] Kent Bye. "XR Ethics Manifesto" Greenlight's XR Strategy Conference. October 18, 2019. [Published on YouTube November 5,2019.] https://www.youtube.com/watch?v=CXgY3YXxqJ8

My other big suggestion is, "Well, are you going to pledge that you will never do certain things?" "Oh no, no. I mean, because we don't know, maybe." Well then you're not writing a privacy policy that is pro-privacy. And that's okay, but let's not pretend otherwise. It'll be interesting to know who it impacts in the XR space.

But getting back to law enforcement, one area that companies try to respond to concerns about government access requests was to do transparency reporting. They were going to put out these really detailed reports about how often and when and where different countries and law enforcement agencies asked for what information.[112] That's something that's evolved over the past ten years. Well, that's still largely just the tech companies that do that and as every company enters into a tech space, there's a lot of people that aren't doing it.

My best example of this is our cars. Police are calling up the smart car people all the time to get information out of cars, to figure out where people were.[113] You've seen some headlines about this with GM's OnStar service being used by law enforcement. And yet the car companies, I think, largely have resisted doing transparency reporting because they don't want people to become aware that this is a real situation.

And you think about heads up displays, AR type of augmentation and self-driving cars, we're going to need much more transparency reporting from everybody. And there tends to be a lot of resistance from this, outside of the core group of tech companies.

Bye: Yeah. I think one of the approaches that Facebook at least has taken with their privacy policy and talking about some of these things is that they'll make the argument – or at least imply that some of this data is absolutely required for them in order for the technology to work. In a lot of cases, that might be true in terms of you need to know what the room is like and how your body is moving. But I guess there's no limits in terms of what they do with that data if they are recording it. And I guess with Project Aria, which was just announced there at the Facebook Connect One, which is this research project to have Facebook employees wear these augmented reality smart glasses that are capturing what they're referring to as "egocentric data capture." So first-person perspective of everything you see or look at or do, it's basically going to be capturing both with cameras, but also correlated to what you're looking at using eye-tracking data correlated to what you're seeing in the world.

Now this is a research project. So it's like a little bit of a sandbox. But I guess the intention is to potentially train what they're calling "contextually-aware AI." So AI that's always aware of what context you're in and what you're doing. And then I could see a future where they would potentially want to do all of this

[112]Facebook Transparency Report. https://transparency.facebook.com/

[113]J.P. Hubaux, Srdjan Capkun, & Jun Luo. (May 2004). The Securityand Privacy of Smart Vehicles. Security & Privacy, IEEE. 2. 49 - 55.10.1109/MSP.2004.26. https://www.researchgate.net/publication/3437601_The_Security_and_Privacy_of_Smart_Vehicles

hyper-aggressive egocentric data capture on a more closed environment to be able to train AI to the point where they wouldn't necessarily need to do all this long-term capture and storage of all this egocentric data capture of millions of people walking around with these Facebook Reality Labs surveillance glasses walking around in reality, but that they want to potentially do this real-time analysis.

And so they'll be processing the data and maybe making inferences based upon real-time – inferences based upon what you're looking at, which I think is the equivalent of what the NSA has done in terms of metadata capture where they're not actually listening to phone calls, but they're just listening to who you call and when, and that extra layer of abstraction of that metadata has different privacy implications.

And what I worry about is that we're moving into a future where there's just going to have a whole load of data that's going to be captured about our eye tracking, what we're looking at, and they're going to be doing these real-time inferences to be able to make judgements based upon what we're saying and doing. And maybe that raw data aren't being captured, but they're able to make these judgments about who we are and what we're looking at.

Jerome: Yes. I mean, look, that may well be the end game. I don't think we're there yet. And I guess my challenge to this industry is – well, what confuses me with XR, as a lawyer, is I don't actually know what information is absolutely needed for the product to work. I don't know what information would be nice to have to make it work better. And what is entirely extraneous. I also note that foveated rendering is both a way to offload processing power to make the technology better, but also opens the door to everything that you're concerned about. What do we do then? I don't think I have a very good answer there. That's actually, I think, where law and regulation should come into play. Let's be honest, we do not have laws and regulations on the books today that are adequate to address those specific concerns.

Particularly, if Facebook somehow discloses it in its privacy policy, there's not really going to be a problem. Now there's exceptions to that. Will the decision be somehow impacting an eligibility determination? Are they going to be profiling where and when you might want to go to – what schools, what employment, what housing you could get? We do have civil rights protections for that type of stuff.[114] That's one area where certain eligibility decisions raise tougher standards and there'll be required to do more.

You'll also want to make sure, and this is another thing where I think we need research. Will there be any disparate impact or biases that relates to protected classes like race or sex? Well, if we see some of those differences emerging, we do have laws that might apply. But in the meantime, we are stuck with what

[114]Civil Rights Requirements - A. Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d et seq. ("Title VI"). U.S. Department of Health & Human Services. https://www.hhs.gov/civil-rights/for-individuals/special-topics/needy-families/civil-rights-requirements/index.html

Facebook's doing now, which is where they released a set of high level innovation principles that sound good at some level.[115] And ultimately, you have to trust Facebook. And obviously, I don't think a whole lot of people trust Facebook, unfortunately.

Bye: Well, part of my frustration, I guess, is that it feels like Facebook is moving into this phase where they've got over 3 billion users. They feel larger and more powerful than any individual government. And yet the ways in which that they have any transparency or accountability for all these different algorithms that they're deploying, or just as an entity. They're not a democratic institution. They're a private corporation. And so, a lot of these discussions that they've been having have been behind closed doors.

I know that they released a white paper a few months ago that was looking at how to do notice and consent a little bit better. But they said they wanted to be collaborating and talking to different privacy experts and people who are in public policy realms to create regulatory sandboxes, to create these experimentation zones, to be able to have the interface between public policy and their privacy policies. [116] And how to find it so that it doesn't just completely ruin user experience. But to have a middle ground there, and to iterate more quickly in a way that it leads to better regulation rather than just something that's going to make a terrible experience for now and – [crosstalk 01:03:13]

Jerome: And doesn't all that sound good to you, though?

Bye: Well, I guess my issue is that they're going to be talking to all these different experts. I'm like, "Great. I want to be a part of that conversation." And as a journalist and someone who wants to report on these things, then I got the distinct impression that I wasn't invited to any of these conversations. That any of these conversations that might be happening would be behind closed doors, under NDA, maybe under Chatham House Rules, but that we have the entity as big as Facebook moving forward and determining some of these policy issues, but in a way that's completely not transparent to anybody to actually be engaged into that process.

Jerome: Look, I think that's completely accurate. As someone that's worked in tech civil society or tech policy for the past eight years, and I've engaged with a number of tech companies, including Facebook. And they all bring in different constellations of stakeholders, consumer advocates, privacy people, domestic violence types of groups to try to talk through products. I think it's always been a challenge on our end about how effective is any of that? Is that just a box-checking exercise for them to say that they spoke to someone?

[115]Erin Egan. "Making Data and Privacy Easier to Understand Through People-Centered Design" Facebook. July 14, 2020. https://about.fb.com/news/2020/07/making-data-and-privacy-easier-to-understand/

[116]"Communicating About Privacy: Towards People-Centered and Accountable Design" Facebook White Paper. July 14, 2020. https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf

And that – I want to be charitable to Facebook. They're trying to do their due diligence in some respects. I think there are people there who mean well, and they have their blinders and sometimes we can elevate an issue for them that they did not understand. That does happen sometimes. I don't think it happens enough.

I don't think it happens in a way that's transparent or really a way that journalists would expect. And so we need to figure out, again, going back to this idea of, well, how do we get third-party researchers and other people engage in a process that's part of a regulatory requirement? How do we do that?

So my organization, Common Sense Media has been involved in this effort against Facebook called Stop Hate for Profit, where we partnered with civil rights groups to push them to do better about some of their content moderation policies that have led to, well, frankly like a toxic environment on Facebook.[117] And I think there is strength in numbers. When we can get journalists, major mainstream publications, or you can find other companies to partner with to sort of –

So here's what I'm trying to describe. As of right now, and I think part of this is bandwidth situation. My day job is not working on XR. There are very few privacy groups, privacy advocates that are focusing on this subject. I mean, this year it's all been pandemic, COVID-19 privacy. So we're very reactive. Facebook comes to us with an issue and wants to talk to us. I think we do a much better job when we're vocal and public about something moving forward. So I pointed to Kavya's work and XRSI creating a privacy framework, as an independent thing that she's then trying to like gain traction for.[118] [119] That's now something Facebook has to react to as opposed the other way around, and I think that tends to have the most effect.

And we've seen this in the context of tech platforms around – again, Facebook, it tends to be discriminatory advertising. Civil rights groups have been very good at forcing Facebook to do things on that front because they have been saying, "Hear our demands, do this." We've seen examples of this in the context of the sharing economy around Uber and AirBnB, where civil rights groups and tech groups have identified an issue and gone to the companies.

And I think that needs to happen with XR. I think the problem of course is just bandwidth. Every minute I spend trying to parse through whatever federal privacy legislation is and what that might mean for California state privacy legislation or Washington state privacy legislation that has zero to do with

[117] Rebecca Heilweil. "Civil rights organizations want advertisers to dump Facebook" Recode. June 17, 2020. https://www.vox.com/recode/2020/6/17/21294451/facebook-ads-misinformation-racism-naacp-civil-rights

[118] "The XRSI Privacy Framework version 1.0" The XR Safety Initiative. September 8, 2019https://xrsi.org/publication/the-xrsi-privacy-framework

[119] Jeremy Horwitz, "XRSI releases VR/AR user privacy framework, citing 'urgent' need" Venture Beat. September 9, 2020. https://venturebeat.com/2020/09/09/xrsi-releases-vr-ar-user-privacy-framework-citing-urgent-need/

what a company might do in terms of mapping, that's a missed opportunity.

Bye: Yeah, I guess that's the concern that I have, is all this discussion around federal privacy, but how much of those XR concerns are being addressed in a way that's going to actually have something that's going to still be relevant in ten to twenty years? So I don't know. You're on the front lines and you're one of the few people that I've met at least that have a fairly good cross-section between what's happening in the XR space and the privacy space, especially at the policy level. But I guess what I see at the same time is more industry trade groups, whether it's the XR Association and –

Jerome: Acronym soup!

Bye: Or you also have this other group – I think it's the Institute for the Future of Innovation – or what's that called?

Jerome: Institute for Technology Innovation Foundation? Oh no, I'm getting it wrong.

Bye: ITFF –

Jerome: ITIF. *[the "Information Technology & Innovation Foundation"]*

Bye: Yeah, ITIF, which is the group that Facebook brought in to develop the privacy policy for the Project Aria.[120] So you have these trade organizations that are advocating on behalf of these big tech companies and they often will want to have the least amount of regulatory burden on them. Or maybe you could just maybe describe what they're saying, what they're line is – because I know you've been tracking this for a while and you kind of tapped into the rhetoric and the arguments.

And then Facebook has even recently been saying that they want a federal law. Maybe that's because they don't want fifty state laws to deal with. But so what are some of the things that you're hearing from some of these industry trade groups? Or groups that are working directly with the big tech corporations when it comes to what they want for privacy?

Jerome: That's a big question that gets real DC wonky real quick. So, A: I think it's important for folks to understand the dynamic that we face right now where trade associations have a tremendous amount of power. And the companies actually make decisions and could be really valuable contributors, but they sit silently in the background and don't do a whole lot.

So we end up fighting with trade associations. Alvaro Bedoya did a really good article in Slate about five years ago already, where a coalition of privacy advocates and consumer groups basically walked out of a stakeholder effort, run

[120]"Facebook's Project Aria Takes Important Step Toward Establishing Data Collection Best Practices in the AR Industry, Says ITIF"Information Technology & Innovation Foundation. September 16, 2020. https://itif.org/publications/2020/09/16/facebook-project-aria-takes-important-step-toward-establishing-data-standards-for-AR

at the NTIA, the National Telecommunications and Information Association.[121] That's a U.S. government agency to work on best practices and a binding code of conduct around facial recognition. And their position was you have these quiet trade associations taking impossible positions, not willing to meet us anyway, not willing to negotiate, not willing to compromise. And the companies might be reasonable, but they hide behind these groups and don't engage.

And I think we're seeing that quite a bit with federal privacy legislation. So I think it's important to acknowledge that the U.S. federal privacy debate has been going on for decades, just decades, as I mentioned up top, but this most recent iteration was started in 2018 by I think the combo of the GDPR coming into force in may of 2018,[122] the Cambridge Analytica scandal in March of 2018,[123] and then the surprise emergence of the CCPA in June of 2018.[124] So everybody started getting engaged in lobbying Congress, and every trade association I had a chat at one point, came out with privacy principles.

I want to acknowledge up top that these privacy principles are better than the privacy principles we would have seen ten or twenty years ago. I mean, even the U.S. Chamber of Commerce now supports a federal privacy law.[125] [126] It's not a good privacy law, but even they are now willing to say we should have a law.

I think the things that I see a lot in these principles and I've, even when talking to these people formally and informally, I'm always telling them, well, you really need to stop leading with people should know more information about their data. Because again, that's code for notices. We're going to do better on privacy policies. Companies, trade associations, they're happy to have a privacy law that just requires them to do a better privacy policy because you can do a better privacy policy in a way that a regulator can say, yeah, you did it or didn't. That isn't going to do anything to make us know more about the information the company is actually doing. It's not going to help the general public in any

[121] Alvaro M. Bedoya, "Why I Walked Out of Facial Recognition Negotiations: Industry lobbying is shutting down Washington's ability to protect consumer privacy." Slate, June 30, 2015. https://slate.com/technology/2015/06/facial-recognition-privacy-talks-why-i-walked-out.html

[122] Thomas Dover "GDPR Compliance Deadline is May 25, 2018" Lexology. https://www.lexology.com/library/detail.aspx?g=9f9818f7-294e-4258-b904-0475506639be

[123] Carole Cadwalladr & Emma Graham-Harrison "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" The Guardian. March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[124] Colin Lecher. "California just passed one of the toughest data privacy laws in the country" Verge. June 28, 2018. https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote

[125] "U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law" U.S. Chamber of Commerce. February 13, 2019 https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law

[126] "Model privacy legislation calling for a federal privacy law" U.S. Chamber of Commerce. February 13, 2019 https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf

real way. So whenever you see anyone say like, "Oh yeah, people should have more understanding." And then they'll say, "Users should have more control over their information." But that control is always really limited.

And if there's one thing I would encourage you and all your listeners to read, it is Dan Solove's article on privacy self-management where he goes through the problems with what it means to have a framework that is based off of giving people more information and more control.[127] It's overwhelming and it absolutely benefits companies because then it puts the onus on users to make these decisions. "If people just know a little bit more and they have the right controls, well then, we don't have to do anything." So all the frameworks start with that.

You are seeing increasingly a recognition that there needs to be some limitations on how information is used. That's where we don't agree on what that means. Does it get at advertising? Does it actually cabin the collection of information? But you do see that.

And then I think another thing that's been new is a recognition that we should also have more security standards in place. Privacy and security are not the same thing. They often get conflated to be the same thing, but they're not. And you can pass a really strong privacy law, and still leave data fundamentally unprotected. And I think that's a real concern that everyone now understands.

And then I think the other big change from industry is just that we need to have more resources for enforcement. Now this gets back to the whole private right of action thing. But if you go back to privacy proposals from ten years ago, it's like, "Well, the FTC has it covered." Now it's like, "We've got to give the FTC a billion dollars." That is new. That is not something that industry was willing to seed in the past. And I think that's absolutely important. Privacy regulations are costly and they require meaningful enforcement.

And my life is spent focusing on the Federal Trade Commission. Federal Trade Commission is a tiny, tiny agency. Most Americans have never heard of the FTC. It doesn't have nearly the resources or ability to get money that new agencies like the Consumer Financial Protection Bureau which was created in the financial crisis, what they can do. It's a nearly as powerful as something like the FCC and arguably depending upon how the political winds blow, it's not really even as powerful as the FCC, which governs a lot of technologies. So it is something that industry is now saying we've got to throw more money at the FTC.

Bye: Yeah. I know that the issue of control, there's a dynamic where most of the default settings of technology just simply do not get looked at or changed.

[127]Daniel J. Solove, Privacy Self-Management and the Consent Dilemma (November 4, 2012). 126 Harvard Law Review 1880 (2013), GWU Legal Studies Research Paper No. 2012-141, GWU Law School Public Law Research Paper No. 2012-141, Available at SSRN:https://ssrn.com/abstract=2171018

And so whatever the defaults are end up being the de facto standard for what is happening.

And I know that after watching the five-and-a-half hour testimony from the four major CEOs from Apple, Amazon, Facebook, as well as Google/Alphabet,[128] [129] that the common refrain was that the data that we're collecting are providing services that are of benefit to our users. And so that's like in order to provide certain services, they have to collect certain data.

In the case of some of these services like Google and Facebook, it's the advertising to even sustain and fund a lot of this. But that seemed to be this trade-off that we have these free services and we're mortgaging our privacy and our data to pay for them. And I don't know if the larger questions around that business model of surveillance capitalism.

I know Shoshana Zuboff, the author of *Surveillance Capitalism* was saying, "Okay, well this is maybe a market that we should just outlaw."[130] So when it comes to the federal privacy regulation, I don't necessarily see anyone going as far as saying, "Okay, this is a market that we should just prevent from happening."

Jerome: No, that's accurate.

Bye: So how does surveillance capitalism get reined in a little bit more on this?

Jerome: So a couple of things. First, I do want to push back on the – "surveillance capitalism" is amazing rhetoric. Everybody has latched onto it. And I get it. It has a rhetorical appeal, and it seems to describe a lot of what we're facing. I mean, there's a new documentary on Netflix called *The Social Dilemma*[131] that really gets at this issue. But I hate to say it, I think that's giving companies too much credit.

And I would encourage folks – Cory Doctorow just published a really good critique of *Surveillance Capitalism*.[132] And what he basically said is we're not really concerned about surveillance capitalism. We're just concerned about what capitalism looks like when we have only a handful of companies that control communications and e-commerce. The magic of what Facebook and Google are

[128] Adi Robertson, "Everything you need to know from the tech antitrust hearing" Verge. July 29, 2020. https://www.theverge.com/2020/7/29/21335706/antitrust-hearing-highlights-facebook-google-amazon-apple-congress-testimony

[129] House Judiciary "Online Platforms and Market Power: Examining the Dominance of Amazon, Apple, Facebook, and Google" YouTube. July 29,2020 https://www.youtube.com/watch?v=WBFDQvIrWYM

[130] Shoshana Zuboff. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, January 2018.

[131] "THE SOCIAL DILEMMA is Coming To Netflix September 9" August 21, 2020. https://www.broadwayworld.com/bwwtv/article/THE-SOCIAL-DILEMMA-is-Coming-To-Netflix-September-9-20200821

[132] Cory Doctorow. How to Destroy Surveillance Capitalism. One Zero Medium. August 25, 2020. https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59

doing. I always think about examples like Zynga. Zynga was a surveillance capitalist.

Everybody's obsessed with Farmville, but it was a crappy product and advantaged after its 15 minutes of fame. But instead, surveillance capitalism is I think really just a moniker for a situation where the Internet is really unique in the sense that it was this amazing global network that was established without rules. It came of age in a really unique point of time. I can't fathom the Internet developing the way it has in today's society. And so it created this wonderful narrative of anybody can do anything on the Internet. You have this virtuous cycle of startups that rise and fall.

But what I think Doctorow does a good job of describing is that at the same time as the Internet was coming into creation, it was also at the same time as we were pursuing in our competition work, a universe that incentivizes merging between competitors, buying out new market entrance, horizontal and vertical integration.

And these were all things that at one point in time were illegal or heavily scrutinized and haven't been for roughly the last thirty to forty years. And that has had huge benefits to the tech companies, has huge benefits to across industries, but in particular, tech companies.

Again, I want to come back to – I think so much of this is really about advertising. I'm riffing from Doctorow, but he's dead on. He talks about the discussion of "50% of my advertising budget is wasted. I just don't know which 50%." Like that's the line in ad tech, but that's not a good way of framing it at all. We don't know if it's even 50% is effective. It could be 0% is effective. And a lot of this, I think is ultimately snake oil.

I know in XR space, we get really concerned about profiling, and we're able to read people's thoughts and emotions. Maybe someday. I don't think we're anywhere close to that. Emotion detection has been something that's really been in the news. And this comes in the context of facial recognition.

You have a lot of these biometric snake oil companies. They're going to sell like police departments, smart glasses that are going to be able to assess whether someone's a terrorist or a threat. That advertising already exists.

But Jay Stanley at the ACLU put up this really excellent report on video surveillance last year.[133] And he's like, "There's no evidence that any of this stuff works." And I think that's true across the board. We are buying into a lot of hype because there are tremendous benefits. And it all sounds like really interesting technology, but I don't think it's really there yet.

And I wish you could be a little bit more critical of everything that these companies are going to want to do. I don't know if that necessarily answers your

[133] Jay Stanley. "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy" American Civil Liberties Union. June 13, 2019. https://www.aclu.org/report/dawn-robot-surveillance

question, but it does get on my riff about how we should be careful about blaming this idea of surveillance capitalism on our current situation.

Bye: Yeah. I was in a webinar discussion yesterday from the Internet Archive on the DWeb – the decentralized web — had a discussion and Cory Doctorow was there.[134] He said that all these companies have been not representing the full truth on all these other different levels, and so why should we be trusting them on how they have these magical mind-reading devices? And I take that point.

But also there's been studies in terms of how many "likes" people make, being able to extrapolate certain psychographic profiles that Cambridge Analytica had. And I think if you just take statistically, like if you're able to take a certain amount of information and really harness into to a very specific number of people, then you could have enough of a shift to actually shift elections, even if it's on the order of tens of thousands of people[135] –

Jerome: Oh, it's totally. I don't have a good answer to this, but I think the way content is amplified – I mean, that's what Facebook reveals is like, it's not so much that it's reading our minds and turning us into a bunch of like insult-throwing psychos. It's surfacing conspiracy theories, misinformation, putting people into filter bubbles, because we have a confirmation bias. If we believe something we're seeing more of it.

This is the great benefit of social media and frankly virtual reality. It's allowing communities to surface and connect with each other.

And so now you're allowing minority groups, but also really crazy minority thoughts to have a platform. And you're architecting the systems in such a way that you're encouraging people to do more of this, and join more of it through segmentation. I don't actually think it's as sophisticated.

I mean, I don't even know if all of the new data streams from XR are going to make the situation better or worse, but it does highlight the fact that the way things are recommended to us by tech companies, what they choose to amplify can be really negative for society.

Bye: Yeah. I saw, there's an article from the IAPP that was talking about how the SAFE DATA Act,[136] one of the federal privacy legislation that was put forth was actually like a combination of other laws, and one of which was the

[134]Mai Ishikawa Sutton "DWeb Panel: If Big Tech Is Toxic, How Do WeBuild Something Better?" Internet Archive. September 24, 2020http://blog.archive.org/2020/09/24/dweb-panel-if-big-tech-is-toxic-how-do-we-build-something-better/

[135]S. C. Matz, M. Kosinski, G. Nave, & D. J. Stillwell, Psychological targeting as an effective approach to digital mass persuasion, Proceedings of the National Association of Sciences of th UnitedStates of America. November 13, 2017. https://doi.org/10.1073/pnas.1710966114

[136]Müge Fazlioglu, "Consolidating US privacy legislation: The SAFE DATA Act" International Association of Privacy Professionals. September 21, 2020https://iapp.org/news/a/consolidating-u-s-privacy-legislation-the-safe-data-act/

filter bubble.[137] [138] And that came up in the hearing today. So there seems to be a whole wide range of different issues with big tech corporations. And there seems to be, as we talk about privacy, then you start to throw in there, like algorithm and transparency and filter bubbles –

Jerome: Right.

Bye: It's like getting even more complicated, in some sense.

Jerome: No agreed. I mean, I think it's impressive that lawmakers are starting to see these connections. It does really get back to like: What sort of transparency do we want? Like algorithmic transparency is another controversial topic in privacy advocacy space because giving someone an algorithm that's a bunch of ones and zeros, giving that to me, that's not useful. I need to know what it actually does. I do think we do need more transparency into how we're being sorted and categorized. Facebook does it to some extent.

You can dig through your settings – that no one does because they don't really care – and you can figure out that they think that I'm a middle-aged man based in – they get some of this stuff wrong. I always loved it. I was categorized by one of the data brokers as a – well, I was younger then – but as a middle-aged person that liked golf. And it's like, I don't even own a set of golf clubs, I think you were confusing me with my father. But we don't have access to that, and I don't necessarily think it's individual users or individuals that need access to it.

Again, I come back to this, we need researchers to be able to see it. We need some sort of independent auditing mechanism, maybe regulators, to understand how these bubbles are being created and what they may mean. And then one of the things I'm always interested in is like, and this is tough. There's a lot of politics involved. Could we identify which of these bubbles we just don't want to have? Are there groups that we just think are bad?[139] I think about companies, like Twitters and Facebooks of the world. They somewhat respect, choose what is amplified. Twitter trending topics. All of these platforms have trending topics now. How is that determined?

Twitter is a good example of this, where a couple of weeks ago they had as a trending topic #Wayfair.[140] What is this? And you click on it, and ends up

[137] Thune, Colleagues Introduce Bipartisan Bill to Increase Internet Platform Transparency and Provide Consumers With Greater Control Over Digital Content. November 1, 2019. https://www.thune.senate.gov/public/index.cfm/2019/11/thune-colleagues-introduce-bipartisan-bill-to-increase-internet-platform-transparency-and-provide-consumers-with-greater-control-over-digital-content

[138] John Thune (R-SD), Richard Blumenthal (D-CN), Jerry Moran (R-KA), & Marsha Blackburn (R-TN). S.2763 - Filter Bubble Transparency Act. October 31, 2019. https://www.congress.gov/bill/116th-congress/senate-bill/2763/text

[139] Nick Statt. Facebook completely bans QAnon and labels it a 'militarized social movement' Verge, October 6, 2020. https://www.theverge.com/2020/10/6/21504887/facebook-qanon-ban-all-apps-pages-groups-instagram-accounts

[140] Wayfair confirms there is 'no truth' to conspiracy theories about human trafficking. Twit-

being a conspiracy theory that gets augmented by the number of people trying to debunk the conspiracy theory. Well, why is that even necessarily being a trending topic at all?

And the fact that the trending topics are often personalized to each of us, and we don't know about how that works. I think having a conversation about what types of content, what types of categorization we do or do not want to have. And companies saying what types of content they do or don't want to put us into, could be one quasi path forward here.

Bye: Well, just to give it more of an XR specific argument, relative to the "snake oil" of the existing systems, is that eventually these companies are going to be able to see everything you're seeing in these virtual environments, whether that's in VR, where it's already in their privacy policy that if they want, they can capture what you're seeing within these virtual environments and what you're looking at. In AR, if you have the correlation between these glasses combined with eye tracking, then they're able to then also make these correlations as to what you're looking at in these different environments. If you have different galvanic skin response, or different emotional detections to see how your emotional sentiment is changing, or pupil dilation, what you're interested in, your cognitive load. There's so much information that you can start to get when you start to have complete control of both the virtual environments, as well as these biometric input from the sensors.

When you start to combine that, you're creating a world where you almost have complete control of what you're looking at, what you're saying and doing. Whether or not they're able to actually excerpt any useful data out of that, the point I think is concerning for me is that they're going to be gathering all this data – as much as they can – to see if they can. There's going to be nothing that's going to be holding them back from trying to create a world where they know everything that we're looking at.

And in terms of speech synthesis and reading thoughts, brain control interfaces are at the point where you can't do speech synthesis unless you have invasive ECoG [electrocorticography] nodes on your brain.[141] But in talking to experts at a neuroscience gathering, within five to ten years, what they're able to do with invasive technologies on your brain now, they're going to be able to eventually do with external, non-invasive EEG. They're going to be able to put a device on your brain and then synthesize your speech. So, turn your thoughts into words.[142] Within the next five to ten years, I think we're going to have viable brain control interface devices that can literally read our thoughts.[143] So what's

ter. July 10, 2020. https://twitter.com/i/events/1281720926682275840

[141]Nicholas Weiler, "Synthetic Speech Generated from Brain Recordings: New Technology is a Stepping Stone to a Neural Speech Prosthesis, Researchers Say" University of California San Francisco, April 24, 2019. https://www.ucsf.edu/news/2019/04/414296/synthetic-speech-generated-brain-recordings

[142]G.K. Anumanchipalli, J. Chartier, & E.F. Chang, Speech synthesis from neural decoding of spoken sentences. Nature 568, 493–498 (2019). https://doi.org/10.1038/s41586-019-1119-1

[143]Nick Statt, "Facebook is working on a way to let you type with your brain." Verge.

that mean to have companies that not only have all this information that we're able to look connected to our emotional responses, but potentially what we're even thinking? [144] [145] [146] [147]

Jerome: You're making me scared. That's very creepy, and you're not wrong. I try to not think about that. We ended up getting focused on Facebook. I think Facebook is a good example of this, coming out from a legal perspective. A lot of what you're describing, I think by and large, would have applications in healthcare and applications for education. That's where you're going to want to roll. I'm not going to have – well, who knows? I know people who have chipped themselves already at their employee's request. I know I'm not going to be drilling into my head for a commercial product initially.

So you're looking at regulated spaces, like health and education, which do have laws – considered antiquated – but there are laws in the books, HIPAA, FERPA, at least in the United States and elsewhere. And one thing I actually think is interesting, and I need to think about more about this, but as Facebook has unified its accounts and all this other stuff, the Facebook account, it's not FERPA-compliant. So when schools, in the pandemic, were racing to do remote learning, and you had teachers teaching on Facebook or YouTube and making their kids communicate with them through social media, that is not good under our existing laws. Under HIPAA, HIPAA has a whole lot of technical, contractual requirements that are required.

We can argue whether they're good or bad, there's efforts to reform them. But I guess my response to you is I wouldn't get super worried until Facebook says it wants to enter those spaces and starts figuring out a way to make Oculus FERPA and HIPAA-compliant. And it doesn't look like that's really what they're doing.

Now they'll be doing some interesting research. And I actually think all of the pie-in-the-sky research that's in the here and now is useful, and we probably shouldn't stop all of that. But I do think we get signals based on what spaces the companies are looking to enter into. And at least for now, they haven't signaled that. I don't know if that gives you any –

Bye: Well, a couple years ago at [Facebook developer conference] F8, they've shown prototypes of it. And then UCSF last year, 2019, this type of research

April 19, 2017. https://www.theverge.com/2017/4/19/15360798/facebook-brain-computer-interface-ai-ar-f8-2017

[144] Josh Constine, "Facebook plans ethics board to monitor its brain-computer interface work" TechCrunch. April 19, 2017https://techcrunch.com/2017/04/19/i-sure-hope-so/

[145] Noam Cohen, Zuckerberg Wants Facebook to Build a Mind-Reading Machine, WIRED. March 7, 2019. https://www.wired.com/story/zuckerberg-wants-facebook-to-build-mind-reading-machine/

[146] Casey Newton, "Brain-computer interfaces are developing faster than the policy debate around them." Verge. July 31, 2019. https://www.theverge.com/interface/2019/7/31/20747916/facebook-brain-computer-interface-policy-neuralink

[147] D.A. Moses, M.K. Leonard, J.G. Makin, et al. Real-time decoding of question-and-answer speech dialogue using human cortical activity. Nat Commun 10, 3096 (2019). https://doi.org/10.1038/s41467-019-10994-4

that's going on, speech synthesis specifically, to be able to do mind reading, essentially.

So they have said – they have declared that they have been looking at this in a research capacity.

Now is there a difference legally, as to whether or not when they declare that it's a product?

Because I have faced the issue where Facebook has been very resistant to ever go on the record about anything about how they're going to deal with biometric data privacy on the argument that they haven't released a product on that yet. Therefore, they're not going to talk about it.

Jerome: That's fair. You're right. There is no firm legal division. But I guess, again, going back to my pleading the Fifth and pleading bandwidth issues, they haven't given a whole lot of thought as to what the implications are because they haven't signaled that they're willing to produce a product that is going to be out there in the marketplace for schools, for hospitals to be buying. But your larger point is a concern. And your larger point that the companies are relatively non-transparent is also a concern.

Bye: Yeah. Well, as we start to wrap up here, I'm just curious, you've expressed some skepticism around federal privacy legislation. I guess I have a similar level of skepticism, but also a hope. I don't think we're going to go as far as GDPR – or at least I want to see something that's at least robust enough to be able to expand out as to be adapted, as we learn more about what the potential harms are for XR.

But I don't know, it feels like we're ten to twenty years behind what other countries have been doing, and whatever we implement is going to be half-baked in terms of what actually we really need.

Jerome: Yes.

Bye: So do you have some predictions? Or how do you expect this to start to play out?

Jerome: Exactly that. The argument that industry folks will make is the fact that the United States is so far ahead in terms of Artificial Intelligence technology, is because our regulations are so far behind. We gave them the space to innovate. I don't know if I believe that 110%. I do think – and we talked a little bit about TikTok – I think the AR arms race, or the AI cold war that's emerging between the United States and China, with Europe playing a really interesting middle role, influenced how immersive technologies develop. I think that's inevitable, when you look at how Chinese society's already deploying some of this technology. I'm not optimistic for the role of law and regulation. I wish I were.

I think Congress has really a important role to play. I think our government has, in many respects, handicapped themselves. Congress has handicapped itself in

ways that are just unimaginable. They don't have the – the stat I always give out is, we talk about how big the federal government is. The size of Congress and congressional legislative staff is the same size as it was in the 1970s. So that just highlights how influential lobbyists have become and how largely ignorant Congress has been on issues across the board.

So I don't know how we fix that in the immediate term. It's going to cost money, and we're facing a financial crisis due to a pandemic. So legislation is going to be really tough. I guess I'm more optimistic – and only a little bit here – in terms of just company engagement.

I take your entire point that it's hard to get these companies go on the record, but I do think as more people get involved and make a stink about things, that might help. More stakeholder involvement will be useful. But in the short term, actually putting controls on technology, it's really, you got to hope that the marketplace will govern the worst and most manipulative uses. And I don't know if it has so far.

Bye: Yeah. And without a viable competitor to Facebook soon, VR market at this point, they're left with being able to drive forward their vision.

Jerome: Yeah, absolutely. I did a quick cursory glance because I come at this as a video gamer, and Valve doesn't really have a specific privacy policy for its headset. Oculus is really all you've got, and nobody else is really competing on privacy. As always, I think we put a lot of our hope and faith in Apple.

Bye: Yeah. Well finally, what do you think the ultimate potential of virtual reality and augmented reality might be, and what it might be able to enable?

Jerome: Oh, I'm interested in this because look, I think there's accessibility uses. The accessibility community in general, in terms of giving people back senses, mobility. This pandemic has given me so much Zoom fatigue. I will not do any more Zoom happy hours. I do not think 2D video hangouts really work at all. So virtual telepresence in the way that people are envisioning, where the audio is different based on distance, and you can actually network. I think there's tremendous utility there. Both in our personal lives, but certainly in the new remote work environment we all have.

And then, sign me up for super smart AR glasses. When you have the ability to navigate the world with a contextual, heads-up display. I come at this in the sense that I live in Washington DC, and everyone is on their phones, just looking at their phones. I've had to pull two people out of traffic because they are walking across as a car is coming. I don't necessarily know if we raise our eyes to the sky with smart glasses, if it solves that problem, but I think it might.

And at the same time, it'll also just be a tremendous, this is a cliche, but a boon for technological innovation. I really do believe that AR smart glasses could be the next platform that's akin to the smartphone.

Bye: Yeah, for me personally, I think there's so many more privacy risks with

AR glasses and the public. And that's maybe why I like the private use case of VR, because I don't expect VR to be out in public.

I want to share one quote that I got from Sarah Downey. She said that "Virtual reality technology could be either the world's worst surveillance technology. Or it could be the last bastion of privacy."[148]

I thought that was actually quite intriguing and provocative because as we go around with facial recognition and everything else, as we're out in the world, when we actually find that we have less privacy than we do in these virtual worlds if – and it's an if, a big if – if we architect it properly.

So I don't know, that's a thought that's been sticking with me. Maybe VR will be one of our last areas where we have true privacy.

Jerome: I think it's a great quote to end on. It does leave us as to, what is the expression, where it's a simultaneous dystopia or utopia. I think that this technology really can be a catalyst for a lot of really important conversations that we haven't had about how the rest of technology is infecting or affecting our real life, physical lives.

Bye: Okay. Is there anything else that's left unsaid you'd like to say to the immersive community?

Jerome: Nope. That's it. Thanks so much for letting me rant at you for two hours.

Bye: Awesome. Well, Joe, thanks so much for joining me here on the podcast and help giving a larger context, not only for privacy in general, but also some of the XR specific concerns. So yeah, thanks for joining me.

Jerome: No, thank you. I hope I wasn't too wonky. Privacy is all I do sometimes, and I worry that I've made it both less interesting, and I haven't figured out a good way of communicating what I do to other people.

Bye: No, it was good. I think, for me, it's the cross-section of so many vital issues here, as we move into the future. So I got a lot out of it. So yeah, appreciate it. So thank you.

Jerome: Thank you. So look forward to staying in touch and pester you on Twitter.

Wrap-up & Take Aways

Bye: So that was Joseph Jerome. He leads the multi-state advocacy work for Common Sense Media.

[148]Kent Bye & Sarah Downey, "#493: Is Virtual Reality the MostPowerful Surveillance Technology or Last Bastion of Privacy?" Voicesof VR Podast, January 13, 2017. https://voicesofvr.com/is-virtual-reality-the-most-powerful-surveillance-technology-or-last-bastion-of-privacy/

So I've a number of different takeaways about this interview is that, first of all, well, just to get the history and the evolution of privacy policies just gave me so much more insight, in terms of the definitions that these companies use are being defined by the laws that appear in the United States. And so it's not like the philosophy of privacy that these companies are developing are independent of what those laws are. They're essentially just following those laws.

So there's also been a lot more talk about what the federal privacy legislation approach would be in the United States. And that's been catalyzed by, as Joseph said, three different events in 2018. In March, there was the Cambridge Analytica scandal with Facebook, and May was the launch of the European Union's GDPR. And then June of 2018 with the California Consumer Privacy Act, the CCPA, which he said was a bit of a surprise. But those things together started to bring this larger discussion about the need for some federal privacy legislation.

And it's a complicated issue. It's not a simple thing, just because the approach for law with the United States has been so narrowly-scoped and just focusing on one little thing at a time, whether that's video rentals, or education, or financial privacy, or health privacy. It's not like a comprehensive privacy philosophy was fully formed, and they just developed all laws from there. It's piecemeal and all these different laws together.

And not only that, but each state has their own laws as well. And so you have to think about how does the federal law interface with the state law, and what point does it preempt it, and is there other sticking points of the private right to action? So giving people the right to sue, if there's harms and transgressions that have been done.

And Joe's big thing is that he wants to have more than one police officer. So rather than just the FTC being the only police officer who's monitoring this – then there's also the state attorney generals for the state level – but there's not a lot of enforcement that's happening. So how do you actually approach that?

And are there ways to have, like Ryan Calo said in his thought experiment paper that he published back on September 3rd, 2013, called the consumer subject review boards. So this idea of having independent researchers work more directly with getting access to all this data. Because the data is very sensitive, it's private, and there's a lot of it. And so to really have any oversight, then you would almost need to open it up for independent auditors and researchers to go in and be able to do that. But Facebook's not just going to let them do that. There needs to be some authority from the government that is making that a requirement for this type of thing to even exist. So Joe says it's likely going to be a potentially useful thing to have independent researchers, who are seeing what those privacy practices are and how well they're being followed. So that could be a part of the enforcement as well.

So there's a lot of different discussions about what that exactly would look like, but there's also just this partisan polarization that happens here in the

United States. And so there's these sticking points, like whether or not there's going to be a private right to action or not. And preemption is this issue for relationship between the federal government and the state government, but there's also other tensions between being able to have innovation happen versus protecting consumer rights to privacy. Those sometimes are mutually exclusive to see how, if you take too much control over the privacy, then it may stop innovation. But if you have too much innovation, then you're not really taking care of your privacy.

So I feel like the pendulum has been on the side of innovation for a really long time, and it's starting to swing the other way. And there's actually a discussion that happened at a Senate committee hearing, it's from the US Senate Committee on Commerce, Science, and Transportation. They had a hearing on revisiting the need for federal data privacy legislation. It actually happened on the day that I did this interview with Joe. So after I watched this whole hearing, then I did this interview with Joe.

But Julie Brill had this really amazing response from Marsha Blackburn as to why we need a federal privacy legislation. And she used to be a Federal Trade Commissioner. Now she's the Chief Privacy officer at Microsoft. I'm just going to play this clip of Senator Blackburn asking Julie Brill why a federal privacy legislation is important.

> **Senator Blackburn:** I want to go back and talk about the impacts. Mr. Liebowitz and Ms. Brill, let me ask you, because you each spoke about what we're up against, if we do not do a privacy standard, and we talked about that in domestic terms. Let's very briefly hit that in what it means globally, if we do not develop a standard. Ms. Brill first, and then Mr. Liebowitz.
>
> **Julie Brill:** Sure. Thank you so much for the question. And also thank you very much for the leadership that you have shown for so many years on this issue, Senator Blackburn.
>
> If the United States does not pass a strong, robust federal privacy law, we will lose our edge in terms of competitiveness on the global stage. And that means both in terms of the global economy, and the ability of companies to engage effectively in the global economy. We will also lose our thought leadership, in terms of where the world is moving, in terms of how people's data should be respected and how it should be treated.
>
> We are seeing many countries adopt laws. In two years, 65% of the population of the world will be covered by privacy laws. And many of these laws are being written with respect to a global standard that the United States is not participating in developing right now.
>
> So we will lose our competitiveness and our ability to engage in the global economy, as well as in thought leadership. We will also, be-

> cause we won't be engaging in the global economy, that is companies won't and other organizations won't be able to engage easily in the global economy, we will lose innovation. We will lose the ability to benefit from ideas around the world, which will augment our ability to innovate.
>
> And then finally, if we don't pass a federal privacy law to deal with these issues, we will have a great deal of difficulty in the United States, in terms of dealing with pandemics like the COVID crisis, in terms of providing people with the trust that they need in order to allow companies, governments, and other organizations to respectfully and responsibly use data to address these crises. So there is a lot that will be lost, and there are great implications if a federal bill is not passed by this body soon.[149]

Bye: So when I heard this response, at first, I was like, that doesn't make sense because why would making all these really tight regulations make us more competitive? It seems like that could stall innovation, but in order to really participate in the global ecosystem of where the world is going, Julie said that over 65% of the world's population will be under some privacy protections that are more similar to the GDPR than anywhere else. And so this just seems to be where the world is going, and that if United States companies are not forced to be able to follow those privacy laws within the United States, then they're not going to be able to compete internationally.

And we're just going to create this Balkanized Internet, which was one of the fears that Joseph had, which was that with these different regulations, you have the risk of starting to break up the Internet in this way, where you don't have an equal opportunity to be able to interact with people around the world. And so by not participating in this larger discussion about privacy, then United States is just not having their perspective be represented.

So just generally looking at all these different issues, the big challenge here is that it has been very fragmented, very reductive approach, and it really takes taking a step back and understanding a holistic perspective of what the philosophy of privacy should even be.

Dr. Anita Allen is a philosopher of privacy, who would be advocating that privacy is a human right. And a lot of the GDPR was taking inspiration from her perspective of treating privacy as a human right. This whole fair information practice principles from 1973 is the seed of where the United States is really thinking about privacy. It's really quite antiquated. And a lot of the companies are following this because it's very beneficial for them just to say, "Okay, well, if all the privacy is just cast within the frame of the Federal Trade Commission's

[149]Testimony of Julie Brill Before the United States Senate Committee on Commerce, Science, & Transportation Revisiting the Need for Federal Data Privacy Legislation, September 23, 2020. https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation

deceptive practices. And so in order to overcome the deceptive practices, we just have to tell you that this is what we're doing. And as long as we disclose it and you consent to it, then everything's cool." Well, that's a concept of privacy that, as Joe said, is pretty antiquated, and that's just not the direction where the world is going.

And also, you have different aspects of the relationship between these private companies and the government. And Joe said that there's quite a split between the commercial consumer privacy versus government privacy, so surveillance that's being done by the government. So there's a lot of different things with the Fourth Amendment that apply to what points can the government get access to specific information, but with the Third-Party Doctrine interpretation of the Fourth Amendment right now, that essentially says all data that you give to the third party is essentially public, and the government can just get access to it if they want. They can just ask for it, or they don't know how to get a warrant, they just get it.

And so that whole hole within the Third-Party Doctrine and the ability for the government to just get all this information without much trouble is a big reason for why the Schrems II passed, meaning that the whole privacy shield that the European Union and the United States used to have has just being completely evaporated because of this impermeable relationship between the governments being able to get access to all this information, because of the Third-Party Doctrine.

So there's lots of different things, in terms of even National Security and federal surveillance and what the concept of privacy are and just ensuring that information that's being shared with these US companies doesn't get into the hands of the US government. Now this is again where there's a lot of hypocrisy that's happening with the current administration, who wants to ban TikTok because the communist party of China can get access to all this private information of citizens.

Well, guess what? That's exactly what Facebook and Google and all these other companies are doing around the world. And so if you want to really have those protections, then there needs to be some consideration of actually passing some privacy law that would merit the enforcement of making sure that all these companies that they want to do business with follow these specific practices. And so it's almost this hypocrisy of the United States not following its own laws, in that sense. It's singling out a single company.

And I think even Sheryl Sandberg from Facebook says they're not really supportive of this type of thing because, obviously, it's going to put a huge target on Facebook for other countries to start to do the exact same thing. So the answer and solution is to come up with better privacy practices and to not just let the US government get access to all this information without much oversight.

So the interpretations of the Fourth Amendment is a complete mess, as Joseph said. So it's an issue that I think there's lots of different people that he referenced

that are starting to look at that. So for more information, look at some of the different footnotes. One in particular that I really like is from Gilad Yadin it's called virtuality reality surveillance from 2017.[150] And he makes a lot of cases that how when you start to look at these immersive technologies, then you get these spatial metaphors that we haven't had previously within these other technologies. And so maybe some of those similar spatial metaphors that have been the basis of a lot of previous laws, maybe we could start to use those metaphors to be able to change how some of these interpretations of the Fourth Amendment work. But yeah, that's a little bit more of theoretical law there, but there's just a lot of issues there with the interpretations of the Fourth Amendment and what that means for privacy.

But it's becoming a real issue just because things like Schrems II pass, and then it creates this disruption from European companies being able to collaborate with the American companies. And so there's these artificial barriers that start to come up. It actually came up within the medical conference that I went to, the Shift Medical Confernce, where they were talking about, "Okay, this could add some real implications for European companies being able to collaborate with American companies on specific issues, especially when it comes to [sharing data in the] medical domain."

And the last thing that I'd just say is that there's all these trade associations that are out there that are going to be speaking on behalf. And I did an interview with the XR Association, which is one of the associations that are going to start to lobbying Congress on different issues. They're creating a coalition of what all the different companies can agree upon. They, at this point, haven't made any clear distinctions as to what they're going to be advocating for or against, when it comes to these federal privacy legislation.

But the companies themselves have just been a little silent and not really vocal on a lot of these specific issues. And that's one of Joe's complaints, is that they've just been hiding behind these trade associations and not really engaging directly. So they're using either these non-profits, these 501(c)(3)s, which are more educational, which is the ITIF, the Information Technology and Innovation Foundation – we couldn't think of the exact acronym during this podcast – but they're working with Facebook on some of these project area privacy issues, but they're a 501(c)(3), which is more of an education nonprofit. There's also a 501(c)(6), which is more of the lobbying, which is what the XR Association is. So we'll be diving in and talking more to Liz Hyman about some of those issues as well.[151]

But generally, I'd say that there's so many different issues here, when it comes

[150]Gilad Yadin, Virtual Reality Surveillance (February 15, 2017). Cardozo Arts & Entertainment Law Journal, Vol. 35, No. 3, 2017, Available at SSRN: https://ssrn.com/abstract=3043922

[151]Kent Bye & Elizabeth Hyman, "#952: XR Association Industry Survey & Lobbying Congress on XR Policy" Voicesof VR Podast, October 13, 2020. https://voicesofvr.com/952-xr-association-industry-survey-lobbying-congress-on-xr-policy/

to ethics and privacy and policy. And I'm going to see if Facebook is going to engage more directly on some of these and more of a dialogue on the record. We'll see. They may point me to other people to be able to speak on their behalf, or, yeah, I don't know.

I just think when it comes to a lot of these issues, there's just a lot of pressure and a lot of attention, especially with all the anti-trust stuff that's happening, that just report came out yesterday, looking at Google, Apple, Amazon, and Facebook. So issues around antitrust.

But also just these issues when it comes to the federal privacy legislation and what are some of the different approaches and all the stuff that's happening internationally as well. So, yeah, that's my hope. My intention is that start to talk to them more directly, just to get their voice into this conversation as well.

[UPDATE: Thanks in large part to how this conversation with Joe Jerome set a historical context, then I was able to convince Facebook to let me do an on-the-record interview with their Privacy Policy Manager, Nathan White about a number of these issues in episode #951 published three weeks after this conversation.][152]

So that's all I have for today. And I just wanted to thank you for listening to the Voices of VR podcast. And if you enjoy the podcast, then please do spread the word, tell your friends, and consider becoming a member of the Patreon. This is a listener-supported podcast. And so I do rely upon donations from people like yourself in order to continue to bring you this coverage. So you can become a member and donate today at https://patreon.com/voicesofVR.

Thanks for listening!

[152]Kent Bye & Nathan White, "#958: A Candid Conversation with Facebook's AR/VR Privacy Policy Manager: New Potentials for Community Feedback," October 30, 2020. https://voicesofvr.com/958-a-candid-conversation-with-facebooks-arvr-privacy-policy-manager-new-potentials-for-community-feedback/