

## SCRIPT - TECHNICALLY OPTIMISTIC - SEASON 2 - EP. 2

**RAFFI VO:** Last week, on the first episode of the season, we talked with Lou Montulli. He invented cookies. And by cookies I don't mean chocolate chip. I mean the pieces of data that are passed from individual websites to your web browser. Cookies enable basic stuff on the internet, like online shopping carts. And Lou designed them to protect your privacy.

**LOU MONTULLI:** Cookies were designed at the onset to be privacy protecting. So, we felt that we wanted to preserve privacy wherever we could. In its core of the cookie is a limitation that doesn't allow it to be shared among various different websites.

**RAFFI VO:** But...

**LOU MONTULLI:** Um, we'll get into a complication with that, that enabled personalized advertising.

**RAFFI VO:** Cookie technology got captured by advertisers. And now, these things track you all around the internet. So Lou Montulli, the inventor of the cookie, is now Lou Montulli, one of the enablers of surveillance capitalism.

**We also heard a little bit from this guy.**

**ETHAN ZUCKERMAN:** My name is Ethan Zuckerman. I teach at the University of Massachusetts Amherst. And...I have a checkered past. I started my professional career as a technologist, as a software developer with a company called Tripod, which did some of the very first user-generated content. We did web page hosting. I had the memorable experience of creating the world's first pop-up ad while at that company, and I've been apologizing for it ever since.

**RAFFI VO:** Yep, that's right. Okay now wait. Before you get angry and blame Ethan for all the times your browser has been taken over by ads, let's hear him out. Because the tale of the ignoble pop-up ad actually is a revealing story about how internet advertising works...and how smartphones and social media changed the game.

**And I can relate to both Lou and Ethan. You see, I also have something of a checkered past. Long before I joined Emerson Collective as their CTO, I was an engineer at Twitter, on the early team that built the platform. Which, by the way, is why I'm not calling it X.**

**CLIP [Raffi]:** *And Twitter is being used in a way to sort of democratize information...*

**RAFFI VO:** That's me, in 2012, talking about Twitter at Berkeley.

**CLIP [Raffi]:** *You can see what's going on in the world. Twitter sort of extends your reach into the rest of the world, and sort of pulls that information back to you. We really wanna connect people around the world with the information that's the most useful to them, at the exact moment that that information is created.*

**RAFFI VO:** The team I led scaled Twitter up in a big way. We turned Twitter into, basically, a utility. The world used to think of a tweet as just 140 characters of text. But my team led the implementation of embedding all sorts of *other* data into tweets. Like the sender's location, their device, and their profile picture.

We wanted to use this data to build richer experiences for our users. We had really good intentions. But, in retrospect, I see now where all this was heading. The data we were collecting back then set the stage for more and more data to be collected.

So, I didn't invent the cookie. I didn't come up with the pop-up ad. But I have to recognize that, to some extent, I *also* had a hand in creating this world, where tech companies extract and sell user data as a business plan.

In this episode, we're gonna take a cold, hard look at social media. We need to figure out how these big platforms treat your data. And, I know, it's real easy to rag on social media, and be cynical about its role in our society. But tech that genuinely connects us to each other is worth fighting for. So we're also gonna explore some ways that social media could change in the future. And to be honest, it feels a bit like I'm paying penance.

**CLIP [Raffi]:** *Right now, something like 250 million tweets every single day, every single week, that's how many tweets flow through the system, and remember, that's only tweets coming in, we still need to replicate and fan those tweets out on the way out...*

**RAFFI VO:** I'm Raffi Krikorian, and from Emerson Collective, this is Technically Optimistic.

[THEME MUSIC]

**RAFFI VO:** Let's make sure we understand the online advertising model that was around *before* social media. Again, here's the inventor of the pop-up ad, Ethan Zuckerman.

**ETHAN ZUCKERMAN:** To understand online advertising, you have to understand magazines, because that's where it starts. You start with the model of magazine advertising where advertisers are constructing beautiful, glossy full page ads. And if you're putting an ad in something like the New Yorker and you're buying a full page ad, you know, you're paying a

hundred dollars per a thousand readers, they're multiplying out the circulation and they're charging to put the ad in front of everybody. The digital industry comes around and says, well we're so much better than that, right? Because there's no way to know whether I flip past the ad in the New Yorker. There's no way to know, does it make an impact? Do I do something with it? Whereas online, we can do all sorts of things. We can guarantee that you saw the impression. We can look to see if you click on it.

**RAFFI VO: Rather than charging a fixed fee for a print ad, online publications could charge by the impression. And that means: each time an ad is actually shown to a user. Or, because everything's trackable online, they could be charged by the click.**

**ETHAN ZUCKERMAN:** You have Google come in in 1994 and essentially say, look, we're gonna do this very differently. We're gonna do it on cost per click. And that does a couple of interesting things. The first thing it does is it tanks the display advertising market. Suddenly, anyone who's trying to sell something can basically say, well, if it doesn't turn into a click, it's no good for me. At the same time as pay-per-click comes into play, we have the rise of user-generated content. And this starts with personal homepages.

**RAFFI VO: And Tripod, where Ethan worked at the time, was a very popular place for personal homepages.**

**ETHAN ZUCKERMAN:** This is user-generated content. It's no longer like a magazine. You can no longer guarantee that it's gonna be very high quality, but there's a lot of it. And the advertisers want to advertise on it because it's cheap. But they don't wanna be super closely associated with it. They wanna have a certain amount of brand protection. And that's where the pop-up ad comes from. The pop-up ad is designed to separate the ad from the user homepage. It is not designed, at least at first, to be annoying, in your face, so on and so forth. It's literally designed to provide you with a little bit of brand protection and brand insulation.

**RAFFI VO: So the most annoying thing about pop-up ads — you know that they pop up and block what you're trying to look at — actually began as a way to separate ads from user-generated content. But things went off the rails.**

**ETHAN ZUCKERMAN:** Now, of course, almost immediately, it gets used in all sorts of nasty ways. You know, there's pop-ups you can't get rid of, there's pop-unders, all sorts of other stuff.

**RAFFI VO: As pop-up ads became more and more annoying, browsers became more and more capable of blocking pop-up ads. Nowadays most browsers have this built in. And ad-blockers are widely available as browser extensions or add-ons.**

**ETHAN ZUCKERMAN:** That, in turn, starts browsers as loyal clients.

**RAFFI VO:** A “loyal client” is a term that Ethan developed, along with his research group at UMass Amherst.

**ETHAN ZUCKERMAN:** So you have this program on your laptop that gives you a lot of control over things. You have savvy users who are not seeing a lot of ads and are certainly not seeing pop-ups.

**RAFFI VO:** Web browsers responded to the explosion of ads by giving users control. The website tries to show you an ad, but the browser steps in to prevent this —on your behalf. This is what made them loyal clients.

**ETHAN ZUCKERMAN:** And then you have a shift to mobile, where the users have a lot less control over this.

**RAFFI VO:** According to Ethan, smartphones opened the door for a whole lot of *disloyal* clients.

**ETHAN ZUCKERMAN:** So let's start with what a disloyal client is. If you've got Instagram installed on your phone, that is a paradigmatic disloyal client. Instagram is written by Meta. It is showing Meta advertising. You have very little control over what advertising you're seeing. That client is hoovering up data about you. It knows which ads you're paying attention to. It's sucking down all that data and then it's using it to deliver new stuff to you and you really have very little control over it. So that's a disloyal client.

So basically we move from an open web where you're trying to do ads as if they were pages in a magazine. You have a war between the advertiser and the user for attention. As we get to the mobile phone, the advertiser is winning. And then the advertiser sort of wins for good once we start getting to the app-based world. And once we're locked into a world where we're using Facebook or using Twitter, we're dead. You have no control over how your information is being tracked, you have no control over your ads. That's kind of the path that we ended up on.

**RAFFI VO:** Social media companies are really good at keeping you on their platforms. The big ones have their own messaging services, so you don't have to leave to send a text. If you're in, like, the Facebook app and you click on a link, you're not sent to your web browser. Your link opens inside Facebook, where clearly, they can see every move you make.

It's all kind of like how a corporate office might have, like, a break room full of snacks, or a gym downstairs. On the one hand, super convenient. But on the other hand...it's kinda what your boss wants.

**It's similar with social media. Many features have the effect of making you spend even more time on a disloyal client. And they've become so good at this, that an app like Facebook effectively *is* the internet for many users around the world.**

**And a crucial piece of this? It's the notorious algorithm.**

**FRANCES HAUGEN:** So the first issue is, we have to actually write computer programs to decide what you should see.

**RAFFI VO:** This is Frances Haugen. She's a data scientist who spent fifteen years in the tech world, working at companies like Google, Yelp, Pinterest, and, starting in 2019, Facebook.

**FRANCES HAUGEN:** Today, the content funnel that Facebook wants to feed you is much, much, much more broad than the content funnel that you had access to back in 2010. Today, for many, many people, their friends and family produce so much less content, that Facebook has had to figure out tricks for filling up your feed, and so they've broadened that funnel of what they might show you.

**RAFFI VO:** So, even though your connections might be posting less, Facebook still wants you engaged. So they have to figure out what else to show you. And there's not just one algorithm, there's a whole set of programs that determines exactly what content to put in front of you. And it's based on your behavior — y'know, like, which things you like, click on, or even look at for a long time.

**FRANCES HAUGEN:** A computer somewhere has to say: How likely are you going to engage with this content? How likely are you going to rate positively this content? And that means you now have to start collecting a lot of data to understand: What does this content mean or what does it mean that you like this content or will likely like this content?

And so there's now a very strong incentive to acquire more and more data on you, to dig deep and deeper to build profiles on you and build profiles on people *like* you, because one of the reasons they might show it to you is you're similar to these other people who liked it. And so that process of going in and estimating, you know, what's the likelihood you're going to put another comment or click through. That process of composing your feed by guessing things about content against you, that's the algorithm that puts together your feed.

**RAFFI VO:** That's fascinating. Can you give us a sense of, like, what's the kind of data that they're collecting, aside from, like, what maybe shows up in my profile? Like, what does it know about me and how's it collecting it?

**FRANCES HAUGEN:** So, some of the data is pretty simple. It's things like, you know, they'll go through and say, these words existed in content that you produced before, or here's groups you joined or groups that you regularly go view content for. Lots of information about you. Not just information about you, but information about your friends, like the people who you interact with, we can synthesize even more information about you by saying, "Oh, you are in a community of people that are like this, or your friends behave in these ways. You might behave in these ways." And Facebook has, in the past, been known to buy data on people. If they could know that you have a high household income, or you have some other kind of desirable demographic trait, you'd be worth more to them in terms of things like targeting ads. They have a history of engaging with data brokers, or even credit card transactions, because, you know, if they can demonstrate this person went on to buy something, like, that's also a thing where they can add value.

**RAFFI VO:** Facebook itself is a giant advertising platform. So, they're collecting data in order to train and power their algorithms, not just to show posts that are interesting to you. But also, all this data means that they are really good at putting the right ads in front of the right people.

**FRANCES HAUGEN:** Facebook has a giant pile of data on you, and one of the things I always encourage people who care about data to do is, you know, you can go and download everything Facebook knows about you. There's a data export tool. You can see — it's actually quite interesting.

**RAFFI VO:** Okay so I did this data export thing. I don't have a ton of activity on Facebook, so I'm gonna go with Instagram. I have to click here to request my data. And then they're going to send me an email. Ok here's an email, with a link to download a ZIP file. Wow, it's several gigabytes. I'm opening it. I would extract it to a folder. There's a lot of stuff here. Here's fundraisers I've joined, shopping activity on Instagram, oh, advertisers using your activity or information.

**FRANCES HAUGEN:** People have no idea what they're consenting to. Digging through, you know, a hundred pages of legalese is not something that anyone does.

**RAFFI VO:** On the very bottom, there's Instagram ads and businesses. Advertisers can use or upload a list of information that we can match to your profile. So what they're saying is like these advertisers have a list of types of people they want to reach and Instagram's like, "okay we can reach those people for you" and then they do it. It's a crap ton! It's, like, not a small list. There are easily hundreds. Travelers choice, Bike Monkey, Burberry, I mean literally this list is like — I mean I haven't even gone down five percent of the list. There are some names like The Container Store or Canon, like huge brand names, and then there are also things I've never heard of like...Epic Gardening. This list is ridiculous.

**FRANCES HAUGEN:** And one of the things that would fit within there is the topicality. These are kinda like the subjects of what they think you're interested in.

**RAFFI VO:** Ah, yeah I see it, yep. “Add topics that are relevant to you.” Oh, this is awesome. Things I am interested in: visual arts, which is possibly true, science fiction, gym workouts, which is also possibly true, fashion, and then hair care. I wonder if beards are involved in haircare.

**FRANCES HAUGEN:** And so that topic model ends up influencing what you get to see or don't get to see, but you don't necessarily know that Facebook has put you in these buckets, and that the world that you get to witness is influenced by them.

**RAFFI VO:** In September 2021, Frances secretly leaked documents from inside Facebook to the Wall Street Journal. Anonymously, at first. We're talking tens of thousands of pages, including internal research reports and employee chat logs. These documents alone were alarming enough to spark Senate hearings.

*CLIP [Sen. Blumenthal]: This month, a whistleblower approached my office to provide information about Facebook and Instagram. Thanks to documents provided by that whistleblower, we now have deep insight into Facebook's relentless campaign to recruit and exploit young users. We now know...*

**RAFFI VO:** Frances brought to light some shocking information. She showed that Facebook had a casual attitude, at best, toward stopping the spread of disinformation. She showed there'd been a rollback in policies aimed at protecting civic safety. And she revealed internal research that showed the company was aware of serious mental health risks to younger users of Instagram, owned by Facebook — which actually changed their name to Meta just a few weeks after all this started coming out.

When she came forward and announced her identity, she became known as “the Facebook whistleblower”.

*CLIP [CNN Anchor]: Now the scathing accusations from a former Facebook executive about how the company...*

*CLIP [60 Minutes Anchor, Scott Pelley]: Her name is Frances Haugen. That is a fact that Facebook has been anxious to know since last month when an anonymous former employee filed complaints with federal...*

*CLIP [CBS Anchor]: Whistleblower Frances Haugen said Facebook chooses profit over public safety. She shared thousands of internal documents...*

**RAFFI VO:** And on October 5th, 2021, she herself testified before Congress.

**CLIP [C-SPAN, Oct. 5 Senate hearing, FRANCES HAUGEN]:** *Good afternoon, Chairman Blumenthal, Ranking Member Blackburn, and members of the subcommittee. My name is Frances Haugen. I used to work at Facebook. I joined Facebook because I think Facebook has the potential to bring out the best in us. But I'm here today because I believe Facebook's products harm children, stoke division, and weaken our democracy. The company's leadership knows how to make Facebook and Instagram safer, but won't make the necessary changes because they have put their astronomical profits before people.*

**RAFFI VO:** She'd go on to testify before parliaments in the UK and the EU, as well.

**FRANCES HAUGEN:** I'm known as the person who brought forward all these horrible revelations. And the thing I always try to acknowledge is very, very little of what I brought forward was, quote, new information to the world. There had been activists, there had been researchers that had been raising almost all the issues found in my disclosures. The thing that changed, though, with my disclosures, was proof that Facebook knew these problems were real, they told the public they were not real. Facebook knew these problems were real and they actively misled the public.

**RAFFI VO:** These disclosures sparked a number of actions by state and federal officials, including a lawsuit filed in October, 2023.

**FRANCES HAUGEN:** 41 state attorney generals and the attorney general for the District of Columbia sued the Meta Corporation over lying about the experience and health of children online, on specifically their products like Instagram.

**CLIP [PBS Anchor]:** *More than forty states plus the District of Columbia, have sued Meta, the parent company of Facebook and Instagram, accusing the tech giant of building addictive features into its popular social media platforms that contribute to a youth mental health crisis.*

**FRANCES HAUGEN:** It's so shocking how extreme the violations were.

**CLIP [PBS Reporter, Stephanie Sy]:** *Phil Weiser is the attorney general for Colorado and helped lead the suit.*

**CLIP [Phil Weiser]:** *After the Frances Haugen whistleblowing testimony, the documents she released, our work accelerated. And for the last two years, intensively, collaboratively, we've put together this complaint. We see a real problem. Meta has lied to people, they've been deceiving people about their platform, they've been marketing to*



*people under 13, and they've failed to protect young people. That's why we're taking this important action.*

**RAFFI VO:** We're gonna return to this lawsuit, and to more about how Facebook and Instagram affect children, in an upcoming episode that's focused entirely on kids. It's a super important issue, with lots going on recently, so stay tuned for that.

**But zooming out . . . Frances' revelations made a lot of people think again about social media's role in our society. To be sure, there had been plenty of reporting about social media's harmful consequences before these leaks. But Haugen reframed many of these problems as problems with the very model of social media.**

**CLIP [Frances Haugen on 60 Minutes]:** *It's one of these unfortunate consequences, right? No one at Facebook is malevolent, but the incentives are misaligned. Like, Facebook makes more money when you consume more content. People enjoy engaging with things that elicit an emotional reaction, and the more anger that they get exposed to, the more they interact, and the more they consume.*

**RAFFI VO:** Frances says she's not accusing anyone at Facebook of deliberately causing these harms. She doesn't think anyone there is, like, actively malicious. But she thinks dangerous consequences follow when the powerful, algorithm-driven technology of social media is too heavily influenced by the drive for profit.

**FRANCES HAUGEN:** So in Silicon Valley, there's a recurrent kind of philosophy around data, which is, yes, there are people who sit there and say, "How can we figure out how to get people to disclose certain kinds of data?" But in general, companies try to figure out how to give you value, and then how to monetize that data later. And so I think in the case of Facebook, it's more of a thing that they want to figure out how to make, Instagram or Facebook, something that you can't separate from. You know, if we don't live in a world where you have to actually show the social costs of how you got your profits, companies will just keep stealing from the social side of their balance sheet to pad their economic side of theirs.

**RAFFI VO:** If you go by numbers that Meta put out at the end of 2023, Facebook has over two *billion* daily active users. And that's just Facebook, not other apps owned by Meta, like the messaging service WhatsApp, or Instagram, which itself has over a billion users.

**These are such big numbers that it reveals something: no matter how troubled we are by any of what Frances Haugen brought to light, it's gonna be hard to turn this ship around. Even if this ship happens to be leaking our personal data.**

**Enter the app called Signal.**

**MEREDITH WHITTAKER:** Signal is the world's most widely used, truly private messaging service.

**RAFFI VO:** That's Meredith Whittaker, the president of the Signal Foundation.

**MEREDITH WHITTAKER:** We offer full end-to-end encryption, which is the technology that is capable of guaranteeing that only you and the people you're talking to are able to see what you're sending, read your messages, you know, see your thoughts. So we think of it as bringing the paradigm of private communication, which has been the norm among humans for hundreds of thousands of years, into the digital age. And we do that as a nonprofit. So again, we're not pressured by investors or shareholders to reduce our privacy commitments because the business model in tech is, you know, monetizing data.

**RAFFI VO:** Before joining Signal in 2022, Meredith was at Google for thirteen years. While there, she led research groups, both inside the company and independently, aimed at tackling the problems of artificial intelligence.

But her relationship with Google soured. In November 2018, she helped organize a walkout of over 20,000 Google employees around the world. There's a lot more to this story, but one instigating factor was Google's contract with the US Department of Defense for what was called "Project Maven".

**CLIP:** [PBS NewsHour on Project Maven]

**[Anchor, Hari Sreenivasan]:** *What was the extent of what Google was planning to do and work with on this Project Maven?*

**[Reporter, Kate Conger]:** *So Google's role in this project has been to create artificial intelligence to do image classification on the footage collected by drones. And so, they were trying to help the Department of Defense mark objects in this footage, to say, this car is a car, this building is a building, this is a person.*

**RAFFI VO:** Whittaker wrote a letter to CEO Sundar Pichai that would eventually become a protest petition. It was signed by thousands of employees. It read, in part, quote: "This contract puts Google's reputation at risk and stands in direct opposition to our core values." End quote.

Google would eventually publicly announce that they ended the contract with the Pentagon. And while Whittaker left in 2019, her interest in changing the status quo in Silicon Valley continues at Signal today.

One way to make sure that user data doesn't wind up passing from a tech company to third parties, y'know like the US military, is by locking down what's known as metadata.

**MEREDITH WHITTAKER:** Metadata is as important as the content of your messages. So, metadata is just information about who you're talking to, who your network is, when you're talking to them, perhaps the location where your phone pinged a cell tower and you sent a message. All of those little bits of information that provide really critical context for your conversations and what you might be doing. So we developed innovative privacy techniques to also protect metadata.

**RAFFI VO:** Metadata is data *about* data. In the case of a messaging app like Signal, the data is your actual messages. The metadata is contextual information. Like who the message is to and from, the location of the people messaging, or who the internet providers are.

But you probably first heard the term metadata way back in the summer of 2013. That was when a contractor working with the US National Security Agency leaked a trove of classified documents. This leak exposed the role that metadata was playing in sophisticated government surveillance programs. And the public had no idea.

I'm talking, of course, about Edward Snowden.

**CLIP [CNN, Don Lemon]:** *Our breaking news this evening is the identity of a man who sent the Obama administration into defend and explain mode this week. His name is Edward Snowden, he's an American former CIA employee and computer technician...*

**CLIP [CNN Anchor]:** *Snowden exposed details of a top secret surveillance program that collects tons of phone and internet data to thwart terrorist plots.*

**CLIP: [CNN, Glenn Greenwald]:** *It's created a worldwide debate over internet freedom and the value of privacy, and the dangers of surveillance...*

**CLIP: [CBS Anchor, Seth Doane]:** *Snowden is believed to have released top secret documents about an NSA program that collects cell phone data and internet communications from US citizens. He says Americans have the right to know about it.*

**RAFFI VO:** When I use Signal, what can Signal see?

**MEREDITH WHITTAKER:** As little as possible. We really can't provide much. We can confirm that a given phone number is registered for a Signal account. So I can say, yes, this phone number is registered. I can't tell you whose phone number it is. I can't do much else. I can tell you when that phone number registered for a Signal account. And I can tell you the last time

that phone number accessed the Signal account. But beyond that, there's very little that we can offer.

We need to operate in the ecosystem that exists. A kind of ecosystem that has developed around the surveillance business model. The collection or creation of massive amounts of data, the analysis of that data to create classifications of types of people or types of consumers that can then be sold to advertisers who have access to these micro targets, et cetera, et cetera. And that's kind of the engine of the platform economy. And that has created messengers that are bolted onto social media platforms. That's created a number of expectations that we may not be comfortable with.

This wasn't a democratically deliberated process. This was a regulatory framework that was very clear that commercial surveillance was okay, was unchecked, that enabled private companies to sort of market a surveillance business model as making the world's information accessible and available, connecting all humans. We know the marketing rhetoric, but this was something that was built up outside of public view and certainly outside of anything we could meaningfully consider democratic consensus.

**RAFFI VO: I mean, when I speak about that trade off, of like users are giving over their data in order to use something for free. Companies then monetize that data. That's not your business model. So then what's the plan to make it sustainable? Or like, where does the money actually come in through all this?**

**MEREDITH WHITTAKER:** Well, we are donation supported. Being a nonprofit for Signal is not, it's not a sort of gesture at our altruistic purpose. It's not a nice-to-have. It's actually a structural safeguard. And it's a structural safeguard because the for-profit business model in tech is monetizing surveillance in one way or another, right? You're going to use it to target ads, you're going to perhaps sell it if you're a data broker, you're going to use it to train your AI models and those AI models are going to produce more surveillance via inference et cetera et cetera, so that's the engine of the tech economy.

So if we were not a nonprofit, there's a very real danger that we would be pushed by the incentives of the profit motive. And I think, happily, we have a large enough user base and that user base is growing, that a small percentage of the people using Signal donating could sustain the organization. But we published something recently that was just being transparent about the costs of running Signal, which I don't think is a narrative that is very clear to the public, because of course for people generally, tech is free, right?

What's obscured there is the incredible cost and incredible profitability of that take-your-data-in-exchange-for-free-apps, surveillance business model, and that incredible cost doesn't change just because Signal is a nonprofit.

**RAFFI VO: More of my conversation with Meredith Whittaker, along with a bunch of very intriguing ideas for how to break free from the current model of social media, after a short break.**

**[MIDROLL]**

**RAFFI VO: Welcome back to Technically Optimistic. I'm Raffi Krikorian. And I've been talking with Meredith Whittaker. She's the president of Signal, the privacy-protecting messaging app featuring end-to-end encryption. And she's talked about how different her company is from the social media platforms. For one thing, Signal is a nonprofit. But also, the encryption protocol used to power the Signal messenger app is open-source.**

**MEREDITH WHITTAKER:** Yeah, I mean, open-source — there's, of course, just many eyes. We don't want people to have to take our word for it. So if you have a question about what the Signal code is doing, go to the repo. There it is. Our cryptographic implementations are also available open-source. And anyone can use those. But otherwise, part of our mission is not just to produce the app, which is great, but it's also to produce leading edge privacy technologies that can sort of spread privacy beyond Signal. And we do that with our protocol, which is now the standard. That's what you see used by WhatsApp. It's now implemented by Facebook Messenger; Google licenses it, Twitter licenses it. It's, you know, it's *the* standard.

**RAFFI VO: That's right, the Signal protocol has actually become the standard for messaging *inside* social media apps.**

**If Signal protocol is taken up by Facebook, then why do I need Signal anymore? I already use Facebook Messenger, why shouldn't I just continue using them?**

**MEREDITH WHITTAKER:** Yeah, you know, that's a great question, right? Signal provides by far the most privacy protection. Facebook uses the protocol, which protects the contents of messages. That means they can't see what you're saying. But of course, let's be real. Meta and Facebook are a surveillance company, right? They collect huge amounts of metadata. They, I'm sure, buy data from data brokers, join that with the metadata. They have models of who you are and how you behave. They know who you're messaging, when, you know, et cetera, et cetera. And Signal is a nonprofit solely dedicated to privacy. We're not bolted on to the arm of a surveillance company. And we protect both metadata and content. Now, I also want to say, I think it's very positive that they're adding encryption to these systems. And it's really important that these infrastructures get secured and that as much privacy harm reduction happens as quickly as possible, given that Meta and other companies just have such powerful access to this intimate information.

**RAFFI VO: Signal was built by a company whose revenue doesn't come from selling ads or user data. And that's an important proof of concept: it is possible to have an app that really does connect us to each other, but operates outside of the surveillance economy**

**So, can we do that...but for social media?**

**We're gonna spend the rest of the episode talking with people who are asking that very question. Like, for example, Mike McCue, who, in 2010, co-founded the app Flipboard.**

**MIKE MCCUE:** We started Flipboard to reimagine a lot of how the web works. We created it as what we call a social magazine. We integrated with Twitter, with Facebook, with Instagram, and you could log into all of those accounts from your Flipboard, and then you could see the best of everything that everyone was sharing across all these different social networks.

Now these social networks, as you know, are not inherently interoperable. They're closed walled gardens. But they all had APIs, and we were able to utilize those to effectively create sort of an early version of an open social web, where you could actually follow anyone, see content that people were sharing no matter what service they were using to share it. And people loved it.

**RAFFI VO:** When developers want to build software that interfaces with Twitter or Facebook, they rely on those companies making pieces of code available to them. That's what's known as an Application Programming Interface, or API.

**APIs enable all kinds of interoperability between apps, like when a "Pay with PayPal" button shows up in a coffee shop's app, or, as Mike is referring to, how social media is built into many apps that show you the news.**

**MIKE MCCUE:** Now, ultimately, those services gradually began to restrict or shut down their APIs, and that whole premise basically started to fall apart. The APIs have been more and more challenging to use and to access and to integrate into any product. In some cases, they don't even exist anymore. But that all started to change when people started to look for an alternative to Twitter and they started discovering Mastodon, which is built on a standard that's been around since 2016, called ActivityPub. And that standard is the thing we were looking for, or wish we had back in 2010 when we started Flipboard. It's a way to create interoperability between social networks and over the last year, we've been very, very focused on integrating activity pub deeply into Flipboard. Bringing down the walls around Flipboard in our own walled garden and integrating, what's called federating, with other services that are using ActivityPub.

**RAFFI VO:** Why are these walled gardens bad? Like, why are they bad for users, why are they bad for publishers? How should we draw all that together?

**MIKE MCCUE:** If you look back to the early '90s, getting online involved signing up for a service like AOL or CompuServe. And these were closed walled garden services. And by walled garden, what we mean by that is if you were on AOL, you could email people who were on AOL, but only those people. That is a walled garden. And those services liked that because if you wanted to leave AOL and go to CompuServe, you'd be leaving all of your connections behind

and you'd have to start from scratch. So, the web changed all that. Anyone could make a website, and anyone could visit that website from any web browser that they decided to use. And that interoperability set up a massive wave of innovation where basically all dimensions of our online life became far richer, far more capable.

So fast forward to today — the walled gardens have reappeared. This time around the connections between people and content. And these are what we call social networks. Following other people, posting, seeing those posts, interacting with those posts...that activity today is owned, exclusively, by a small number of very large companies like Facebook, and, you know, X, what was Twitter, and it's very hard to switch to a new service because you have to go build a whole new set of followers and you have to follow a whole new set of people if you try to join a new social network. This is the difference between kind of a walled garden model, like we see today in social networking, and then what I think will be an open model for social, the ability to have all this interoperability, the ability to own your own personal connections on this social web in this fediverse.

**RAFFI VO:** So like, the vision of the world that you want to see it is that, like, we all just speak the same language. And then something like Flipboard can like float across all of them? Is that —

**MIKE MCCUE:** That's exactly right. That language is called ActivityPub. That is a protocol that was created in 2016, that is analogous to, let's say, an email protocol or the web protocol HTTP. But what it does is it specifically focuses on the connections between two different accounts and the way that they post and how people can engage with those posts and reply, comment, favorite, and so any service that uses ActivityPub can connect with these users and access this content.

**RAFFI VO RT:** Where does user data go in this fediverse world?

**MIKE MCCUE:** Well, the user data is owned by the user. You know, you use a server to access the fediverse. You create an account on that server. What is very, very important, though, that's different, is that users have choice, where they can decide that if they don't like the server that they're on they can just simply move to a different server and bring their data with them. So that ownership of the data is incredibly important because today, Twitter or Meta or TikTok, they own all of the followers and following relationships that you've established in that app. But here, you own that and you bring that with you wherever you go.

And for users, what they'll start to see is: they'll be able to move between different providers without having to worry about having to rebuild their whole follow-graph. They'll be able to try new kinds of apps and experiences out that are integrated with ActivityPub into the fediverse. They'll find new alternatives that are built on these open standards. And over time, I think, that will become the standard for how we connect with other people online.

**RAFFI VO:** Okay, so that's the fediverse. And if Mike is successful, it could mean that, whenever you join a new platform, all your followers, friends, and connections from whatever social media you're already on come along with you.

It could mean that you're given control over what data you share, and what posts you see, rather than just being subject to the whims of King Algorithm.

It's the kind of thing that even Meta is taking seriously. This past March, the company announced it was taking steps to bring Threads to the fediverse. So, there's no question: this fediverse thing is a big idea.

Ethan Zuckerman has got sort of another idea. Actually he's got a few ideas. But the first one is what he calls the "pluriverse."

And don't write it off if you hate the name. I don't know why everything has to be called some kind of verse.

**ETHAN ZUCKERMAN:** So the pluriverse basically looks at this idea that we can't wait for Twitter and TikTok and Facebook to go away before we have the social media we want. We have to understand that there are going to be major players in this environment for times to come, but that we need other platforms out there.

**RAFFI VO:** Other, smaller, platforms. In fact Ethan and his lab use the term VSOP — very small online platforms.

**ETHAN ZUCKERMAN:** And so we've been developing a platform, we call it Small Town. It's a social network designed for conversation about local civic matters in small towns.

**RAFFI VO:** It's currently up and running in Amherst, Massachusetts, and Ethan says it's full of lively debates.

**ETHAN ZUCKERMAN:** There are rollicking discussions about whether North Pleasant Street should be turned into one-way rather than two-way, or where we should cite the new public school. We lovingly refer to it as the world's most boring social network.

**RAFFI VO RT:** Okay so actually that sounds like it's a feature, not a bug.

**ETHAN ZUCKERMAN:** Yeah. And you won't be surprised that there is less traffic on that network than there is, say, on Instagram. And so what that means is that if you are using both Instagram and Amherst Small Town you're gonna get overwhelmed by Instagram.



**RAFFI VO:** And that's sort of by design. Ethan's bet is based on the idea that, if we really start using social media to enhance our relationship to our *actual* social network, we'll realize how overwhelming it is to be on platforms like Instagram or Facebook, each of which has a user base in the billions.

**ETHAN ZUCKERMAN:** There is a subset of people who are learning a whole lot about being organizers from participating in online spaces and getting to the point where we could use these tools and learn how to govern within them might actually be a really interesting civics lesson.

**RAFFI VO:** And Small Town is not Ethan's only idea for reimagining social media. Remember the loyal client? It was a term for software that enables users to control data — like an email client with controllable spam filters, or a web browser with a configurable ad-blocker. What would social media look like if it worked like this?

**ETHAN ZUCKERMAN:** Let's imagine for a moment a loyal client. A loyal client would let you do a couple of things. First, it would not just work with Instagram, it could also work with Reddit and Twitter and LinkedIn and anything else that you want to look at. You would control what information you were giving back to those servers. So rather than being subject to Instagram's algorithm, which might decide you will look at influencers now — influencers are more important than your family and friends, they're gonna be at the top of your feed — you could look at this and say, you know what? Today, don't show me any politics and emphasize the number of cute animal pictures I'm seeing. And you could make those choices and that would be delivered to you.

**RAFFI VO:** Social media with this level of user control sounds too good to be true. But Ethan's actually building it.

**ETHAN ZUCKERMAN:** I am trying to develop a new model of social media based around much, much more user control and many more platforms, not just the Twitters and the Facebooks, but lots of small social media platforms run by communities, run by groups of friends, that we govern ourselves and algorithms that are transparent and auditable rather than being these sort of secret black boxes that no one ever gets to look in.

We have a product called gobo.social. It is well on its way towards doing this. This is all open source code, so it's all reviewable. We're also doing the algorithms in ways that they are auditable. So you can actually go and see what the outputs of the algorithm is. You can feed it some posts and sort of see how it scores it. It's a tool that gives you an awful lot of control.

**RAFFI VO:** But are people really gonna be into this?

**ETHAN ZUCKERMAN:** Users may just not want to do it. Facebook and such put amazing amounts of time and effort into making their products frictionless. And even if you have beef with

what these products are doing and how they're doing it, they're really good at delivering user experience. And it is possible that either users don't want the level of control that we think, or that we cannot make something as beautiful and easy to deal with as Facebook, Twitter, et cetera, et cetera.

**RAFFI VO: And that, too, is sort of the point. It's education and training for a future in the pluriverse.**

**ETHAN ZUCKERMAN:** We are moving into a world where algorithms are just increasingly important. How do we understand algorithms and their influence on us and on the world? It's based around essentially saying, "Okay, let's make social media work for you. We're gonna start out with the best guess of what you might want, but you need to do the work of training these outputs. You can make the decision about how you're interacting with your social media." We want it to be educational. We want it essentially to be training wheels for interacting with an algorithmic society.

**RAFFI VO: And I think Ethan's right. With social media algorithms, our behavioral data are the inputs. And the algorithms are trained on that data to generate certain outputs. The more acquainted we are with how those algorithms get from A to B, the better prepared we'll be to understand the world around us. That "algorithmic society."**

**Like it or not, we're gonna have to coexist with these things. And we need to understand what they can do — and what they *cannot* do.**

**JONATHAN ZITTRAIN:** Digital privacy has been such a fascinating and, I suppose, terrifying phenomenon to explore and pursue over the years.

**RAFFI VO: Here again is Jonathan Zittrain, professor of public policy and computer science at Harvard, and, actually, my former professor.**

**JONATHAN ZITTRAIN:** You know, Facebook filed a patent years ago for a method of predicting life events in people, scraping the kinds of data that Facebook scrapes, including the death of a loved one or a pet, or falling in love with someone else, all this kind of, you know, sci fi sort of stuff. And to know that could mean that people in a moment of weakness, they know you have just been laid off from your job, they know you're angry, well, what kind of ads, what kind of things should they push you to do? For the most banal of purposes, just to like, sell one more bottle of liquor.

What if instead they were like, hey, you know, you could probably use a helping hand right now. What can we do for you? We're already treating, and this is starting to inch into AI territory, these like assistants and dialogic companions. They are structured to be, and they are at their most effective, like they give you the answers you want, when you treat them like your friend,

but they are not your friend. They could be. You could try. They might be a bad friend, but you could establish ground rules that say they've gotta be looking out for you. But that's not the ground rules right now. And that is, I think, a really interesting and pressing private and public policy issue.

**RAFFI VO: Jonathan's big idea for a new kind of social media comes down to this: What if social media companies had to act sort of like your friends? Or, really not like your friends, but as what he calls "information fiduciaries".**

**JONATHAN ZITTRAIN:** It was Jack Balkan, a law professor at Yale. He said, you know, I've been thinking about this concept that I'm calling "information fiduciaries". And the idea is that when you meet with a doctor or your lawyer and you share information with them and they give you advice, they don't just have the duties of a business not to defraud you. They have heightened duties. They have duties of confidentiality, of loyalty to you, where if their interests for some reason diverge from yours, they have to put your interests first. They're not supposed to prescribe you a drug because they get a commission if it's not the right drug for you, all sorts of things like that. And the duty arises because of your vulnerability to them. There's an asymmetry.

**RAFFI VO: Yeah.**

**JONATHAN ZITTRAIN:** And ditto for a lawyer when they're giving you advice about something. If we were to impose or ask that these platforms, that they undertake, the kind of fiduciary duties that doctors and lawyers have, given their power and our vulnerability to them and our expectations of them as our friends. Exactly what the parameters of those duties would look like I don't think are yet as obvious as they are for doctors and lawyers because there's been a lot of years to work it out. And you know, I'm working on that list.

**RAFFI VO: This would be a radical departure from the corporate model of social media, and from the profit motive. And that alone seems difficult to pull off.**

**But as Jonathan points out, we might have to tackle what perhaps is an even harder problem first. We have to figure out what we want.**

**JONATHAN ZITTRAIN:** First, we don't know what we want. Second, we don't trust anybody to give it to us. And third, we want it now.

**RAFFI VO: [LAFF]**

**JONATHAN ZITTRAIN:** What it means to put a user's interests ahead of your own depends on a user's own conception of what they want. Just like expectation of privacy, what is your expectation of loyalty? It would be really helpful to get some sense from people of what they do

think of as being loyal to themselves. And I've been working with a great group of folks on being able to ask people their views on different hypotheticals, and then to have that be a starting point for setting the boundaries of how companies should behave. And if they're going to behave differently, at the very least, they need to really, in a non-fine print way, say so.

**RAFFI VO: One of these hypotheticals involves thinking about how rideshare prices are calculated.**

**JONATHAN:** How would we feel if the pricing you're quoted on an Uber ride is partially a function of the remaining battery life of your phone? On the theory borne out by A-B testing, that when you're about to run out of battery, you just want the ride. You're not going to be like consulting Lyft and comparing prices. That is not a privacy violation in the traditional sense because your battery life is not a sensitive data point about you. It's always changing. But it does feel like not fair play. But what makes it unfair? What is that telling us about ourselves?

**RAFFI VO:** If we bring this back to social media for a second, so like, how do we actually plot a path to get some of these ideas implemented in the world, is maybe what I'm really asking?

**JONATHAN ZITTRAIN:** Well, I think that is such a great question. And the fact that there's not an easier, pat answer to it makes it all the more interesting and urgent. I'm part of something we're just spinning up now called the Applied Social Media Lab at Harvard for which the purpose is: What if we decide something different, with approximately two decades of hindsight, and see if we can do better than what appears to be the equilibrium for like, oh yeah, okay, social media, I know what that's like. Is it Twitter you're talking about or Facebook or is it TikTok? 'Cause that's pretty much all there is. And really, is there just no other categories of ways of building how humans can interact and share ideas or problems with one another? I bet there are other alternatives, maybe that is going to lead to different results. If you just throw something out there and say, "Hey, how about instead of using Twitter, use this?" it doesn't work. But if you frame it in a different way, it might be, especially as people are starting to feel generally hung over about social media, that they're ready to try just a different mode.

**RAFFI VO: Frances Haugen agrees.**

**FRANCES HAUGEN:** There has been a presumption I think, going back since the dawn of these products, that people, quote, "can't understand" and so they should just trust the experts. And so overall, I think people do not understand, but we shouldn't work from the assumption that they can't understand because when we begin from the presumption that people can't understand, we, basically say, "Hey, we have to do technocratic solutions to problems, right? We have to listen to the experts and just have the experts come up with solutions." And I think we'll have trouble actually building consent in the population around online governance. Like people will be resistant if they don't feel like they were brought along for the ride.

**RAFFI VO:** Frances also thinks that we can channel the growing popular distaste for the way social media currently does business into change. And government regulation could be a part of that. At least, that's what members of Congress were saying back in 2021, after hearing her testify.

**CLIP [Sen. Ed Markey, from Oct. 5, 2021 Senate hearing]:** *You've asked us to act as a committee. And Facebook has scores of lobbyists in this city right now, coming in right after this hearing to tell us, We can't act. And they've been successful for a decade in blocking this committee from acting. So, here's my message for Mark Zuckerberg: your time of invading our privacy, promoting toxic content, and preying on children and teens is over. Congress will be taking action. Thank you, Ms. Haugen. We will act.*

**RAFFI VO:** But that's proven to be challenging. The US still hasn't passed a federal data privacy law. Congress is still debating how to best protect children online. And, as of this taping, lawsuits that could find Facebook liable for harm are still ongoing.

**We'll talk more about all these things in upcoming episodes this season. But, according to Frances, government regulation isn't enough, anyway.**

**FRANCES HAUGEN:** Most other industries are not kept safe just because a government regulator keeps them safe. They're kept safe because networks of concerned citizens. And investors and litigators and insurance companies and like a whole bunch of different people with different interests are all acting in concert to keep them safe.

And so if we start from the presumption that only, you know, smart techies can understand what's going on, we're never going to try to actually build out that ecosystem of accountability to help us build social media that we can feel good about. And the core project my non profit, Beyond the Screen, has been working on for the last year, we're putting all this effort into helping people to understand, like: Where does an online harm come from? What are the different ways you can address problems? Is to give them a sense that even things we know about today, we have an abundance of solutions, but there aren't the incentives in place to motivate people to actually use them.

And to be clear, some of these interventions are not going to be software. It's going to be things like empowering schools. But one of the ways that we can build out of this is establishing what is the minimum amount of data we need out of these companies in order to do accountability, to do governance. And we call, at Beyond the Screen, we call this the "minimum viable queries". What's the minimum amount of data we need to know the magnitude of each harm on these platforms? And what's the data we would need for each lever to understand if platforms are using the opportunities they have available to them? And that's a very different way of thinking about how do we move forward.

**RAFFI VO:** One of the things I valued most about talking with Frances Haugen is the way she spotlights this unfortunate belief that many of us have almost by default, that somehow, the way social media is right now is inevitable. And the tech companies who have made social media the way it is are untouchable. That we should let them manage their own products because, y’know, “they’re the experts.” It’s a stance we hear a lot.

**But let’s hear Frances out. Because she reminds us that we don’t have to think this way. Social media doesn’t have to be treated like some mystery.**

**FRANCES HAUGEN:** When we mysticize things, you know, when things are mystical, they can be outside of our reach. And I do hope we can demystify these things. Because the way democratic accountability works, you need to have people believe that they can make a difference. And the reality is, you can make a difference.

**RAFFI VO:** Now, that’s what I’m talking about!

**Next week, on Technically Optimistic... we’re talking about how your data is used.. by political campaigns...**

**[CLIP]** Tara McGowan: *There’s so much data and this is all enormously valuable...*

**From people who’ve been inside them...**

**[CLIP]** Dan Wagner: *I mean, in 2012 it was a massively organized field operation of hundreds of thousands of volunteers*

**And have seen how the sausage is made...**

**[CLIP]** Lindsey Schuh Cortes: *Like we look to find twitter handles and match those at the individual level.*

**That’s next time... on Technically Optimistic.**

**[CREDITS]**

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

**If you’ve enjoyed the podcast, please rate and review us – and subscribe on Apple, Spotify, or wherever you get your podcasts. Follow along on social, @emersoncollective.**

**And sign up for the Technically Optimistic newsletter! You'll get my thoughts about the week in tech, with lots of big questions, interesting links. And, you know, tons of ways to get in on the conversation. Subscribe for free at [technically.optimistic.substack.com](https://technically.optimistic.substack.com).**

**I'm Raffi Krikorian. Thanks for listening. See you next time.**