Gaslit Nation Transcript

2 August 2023

“Cindy Cohn of the Electronic Frontier Foundation on Big Brother”

https://www.patreon.com/posts/cindy-cohn-of-on-86982799

[advertisement]

[intro — theme music]

Andrea Chalupa (00:42):

Welcome to *Gaslit Nation*. I am your host, Andrea Chalupa, a journalist and filmmaker and the writer and producer of the journalistic thriller, *Mr. Jones*, about Stalin's genocide famine in Ukraine: the film the Kremlin doesn't want you to see, so be sure to watch it. First, a couple announcements. We are running a very special summer series called “The Future of Dictatorship. What's Next? And Ways to Resist”. This series features leading voices on the front lines of understanding AI, corporate surveillance, Silicon Valley greed, and more, because the dictator's playbook remains the same, but the technology they have to oppress us keeps changing. You can learn more about the dictator's playbook in the *Gaslit Nation* graphic novel, *Dictatorship: It's Easier Than You Think*. You can join me for a special night out in New York City to talk all about the making of that book on Saturday, August 5th at 4:00 PM at the fun Lower East Side bar, Caveat, where I will be in discussion with the comedian, Kevin Allison, of the hugely popular *Risk* storytelling podcast.

Andrea Chalupa (01:42):

If you're not in New York, you can join us by livestream. This is a huge deal for me because I hardly go out, so this will be like a Gaslit *Nation* prom night. Join me at Caveat on August 5th in New York. Signed copies of the *Gaslit Nation* graphic novel will be available for order at the event. For details on how to join us in person or livestream, go to gaslitnationpod.com and you'll see the link right on our homepage with more information about the event. Go to gaslitnationpod.com. That's gaslitnationpod.com. We'll be back with all new episodes of *Gaslit Nation* in September, including a live taping with Terrell Starr of the *Black Diplomats* podcast reporting from Ukraine. That's right, Terrell's gonna be in Ukraine, and we're gonna hear all about his summer, his reporting trips, what he is learning, who he's talking to, and what's next. That live taping will take place on Tuesday, September 12th at 12:00 PM Eastern for our supporters at the Truth-teller level and higher on Patreon. Come join us for that and drop questions in the chat and hope to see as many of our listeners as I can on August 5th in New York at Caveat for a fun night out. Before we get to this week's guest, here's a quick word from our sponsor, Judge Lackey, the wiley narrator of the new *Gaslit Nation* graphic novel *Dictatorship: It's Easier Than You Think*.

[clip - Dictatorship: It’s Easier Than You Think trailer]

Judge Lackey (03:00):

So you wanna start a cult, Every great dictator has one. Learn how to get the money, get the power, get the women by starting your own cult today. Read the bestselling graphic novel from those heathen ladies at Gaslit Nation dictatorship. It's easier than you think. Almost too easy.

[end clip]

Andrea Chalupa (03:22):

Now, meet this week's guest. Cindy Cohn is the Executive Director of Electronic Frontier Foundation, the leading nonprofit defending digital privacy, free speech and innovation. She also worked for a year at the United Nations Center for Human Rights in Geneva, Switzerland. In 2018, *Forbes* included Ms. Cohn one of "America's Top 50 women in Tech". *The National Law Journal* named Ms. Cohn one of "The 100 Most Influential Lawyers in America" noting, "If Big Brother is watching, he better look out for Cindy Cohn."

[transition music up and under]

Andrea Chalupa [00:04:00]:

So on *Gaslit Nation*, we're always saying how the dictator's playbook is the same but it's the technology that changes, which is hard to anticipate. So could you give us, in this age of Elon Musk's Twitter, what in your view is the current state of safety on the internet, where do you think things are headed, and what can we the citizens do of any country to sort of push back at what appears to be… there very clearly seems to be sort of an oligarch consolidation of control of our internet?

Cindy Cohn (04:35):

Yeah, I think that we have some tools that we've used in the past to deal with, you know, say, trust busting and things like that, and it's time we start doing them. I mean, we've ended up in a world in which we have, you know, five big tech companies that control most of what we get to say and do online, and that's just not healthy. I think that the tools of recreating competition, whether that's bringing antitrust law to the digital age in a way that makes more sense, revitalizing the kind of accountability that we might have through other laws that are impacting competition—I'm thinking about the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act and the kind of embrace of a terms of service click wrap world in which we don't own anything.

Cindy Cohn (05:26):

We just license stuff on terms that can change—they're all playing a role in limiting the places that we can engage in online and the security and safety that we have while we're there. I also think that corporate risks aren't the only risks. You started by talking about authoritarianism, so I think it's really important to note that we built the world's greatest surveillance machine in the internet and we are using it to surveil ourselves at a level that is really, you know, kind of breathtaking and is leaking into the physical world as well. It's not just the tracking of everything we do online and access by the NSA and the FBI, but the kind of Ring Nation doorbell cameras, the license plate readers, all of these kinds of things that can be and have been marshaled as tools of repression in various places.

Cindy Cohn (06:20):

And I think we're not really looking at the whole problem if we're only talking about corporate surveillance and we're not also talking about government surveillance and efforts to undermine our security. And, of course, they're not separate because the government buys tons of information from these companies about us and uses it for things like deciding whether we get access to welfare, deciding whether people get arrested or not, and all sorts of other things. I think even maybe perhaps in a wider aperture than you frame the question about what we have to do to stop authoritarianism.

Andrea Chalupa (06:54):

Definitely. And obviously it's surveillance capitalism. What is the current state of surveillance tech? How often are we being spied on? How constant is it? It’s not just our searches being monitored, but what does it look like today for the average person, American, let's say American, going about their business? How often are they watched and in what ways?

Cindy Cohn (07:18):

I think you'd almost have to flip it around and talk about the times in which data about you is *not* being collected. They're pretty small. If you use WhatsApp or you use Signal then the end-to-end connection, the things that you're saying to other people, are encrypted. If two people are using an Apple device then their messages are protected. But otherwise everything you're doing online is being tracked and analyzed. Inferences are being made from it. And then much of that information is being gathered up and sold on a lot of different markets. Some are about advertising, but the police participate in these markets as well. So do foreign governments. So you almost have to flip it around. I don't think there's very much that we do in our lives today that isn't being tracked in one form or another. Now, that's not the same thing as, you know, necessarily like each of us has an individual little policeman following us around. In some ways it's worse because it's the kind of massive all the time surveillance and then, again, feeding it into AI and machine learning systems to make inferences about us in some ways is far more pervasive than the kind of old school gumshoe surveillance.

Andrea Chalupa (08:36):

Yeah. And you mentioned Apple. Does Apple provide in the security features that you think are sort of better than average?

Cindy Cohn (08:45):

In some ways, yes, but it's complicated. I think Apple… We think that one of the areas where we have far too many choices is in app stores and so we definitely have issues with Apple around that, but Apple did pioneer the idea that when you shut down your laptop, everything gets encrypted and you need a password to open it up, which means that if you lose your laptop, you don't lose all your data. Now, Android, you know, Google has followed and other makers have followed, but Apple led in that. Again, the iMessages being end-to-end encrypted in between, you know, from one iMessage to another is something Apple's done for a very long time and it's just built in. And there's some other kinds of device security that Apple does. They have moved away from other things that they were doing that were against security. They've dropped plans to basically scan people's backups and scan systems. So unfortunately I don't think you can pick a winner among Google, Apple, Facebook, Amazon and Microsoft. It's kind of, you know, nobody's great but among them Apple's done some good things and, you know, we try to call 'em as we see 'em. We try to praise a company that does the right thing and criticize 'em when they do the wrong thing.

Andrea Chalupa (09:58):

And what is your opinion of the current debate in the US over banning TikTok?

Cindy Cohn (10:04):

Well, I think it's a pretty dumb debate, I would have to say.

Andrea Chalupa:

[laughs]

Cindy Cohn:

I think that the concerns about the fact that there is all this data being collected about what you do on social media are real. EFF has tried and worked hard to try to get comprehensive privacy legislation passed and to go after the surveillance business model which, of course, the money that drives all of that tracking. But the plan to just try to ban one app, really, it's not gonna work. It's kind of counterproductive and it's not the right way to go about the problem. We need comprehensive privacy law. I mean, it's not like the Chinese government can't go on the same markets that the FBI goes on and buy access to data about what we do online. There is a very thriving market of data about all of us and what we do online that is available to them.

Cindy Cohn (10:53):

So simply cutting off one app, even if they could do it—which I'm not sure you can do it either legally or as a practical matter—isn't gonna solve the problem that the people who are putting forth the TikTok ban wants. I don't have any direct information but I know Facebook was trying to get some heat off of it, and they spent a lot of time on Capitol Hill saying, you know, “Don't look at us. We're an American company. Look at this Chinese company,” and seems to have fed some anti-China sentiment that exists in Washington DC and other places. You know, Montana has banned TikTok as well. But it's really not the right way to go about the problem that people have identified and I don't think it's gonna work. But it's a lot of energy being spent. There's so many problems that need fixing and whenever our attention gets shifted to this bright, shiny, dumb thing that the government wants to do, it means we can't do the real work we need to do to try to make everybody secure, try to make everybody safe online. It's a sideshow.

Andrea Chalupa (11:51):

If somebody wanted to go to this marketplace that you mentioned and see what of their data is available, could they do that? How could they go about doing that?

Cindy Cohn (12:00):

I think it would be pretty hard. A lot of it is aggregated information. And so we are sold not as individuals as much as in little slices, so it's complicated and it's a big, huge market. So I'm not saying there isn't some way that you could get information about you individually. You probably could. But it really isn't sold as an individual thing. It's sold as, you know, “I want all of the people who live in Kansas City who have dogs and might be inclined to vote Republican.” And you'll get a swath of that information so that you can hyper-target at them. That's kind of the model of it. So again, I'm not sure whether you could go and extract personal information about you, but I doubt that you probably could in any way that was meaningful. But that doesn't mean that information about you isn't being collected and analyzed and organized in order to decide whether you're gonna get a mortgage, whether your kids are gonna get to stay with you when Child Protective Services comes, whether you're going to get arrested, what you're gonna get charged for the things that you buy.

Cindy Cohn (13:06):

So that information is definitely going to be used in ways that you can't control and that are gonna impact your life, even if you can't reverse engineer it and get, like, a download of all the information somebody has about you.

Andrea Chalupa (13:20):

Who are some of the worst offenders of spying on people online? Is it the US government, other governments? And you touched on this a little bit, but what are some of the ways they could really take advantage of you in having this surveillance?

Cindy Cohn (13:33):

Well, I think that the US government has been extremely hostile to strong encryption and real security for a very long time. And now the Australian government and the UK government… I mean, basically law enforcement in a lot of places is extremely hostile to basic security needs that people have. I think their approach is, you know, if you're a criminal, they wanna make sure they can catch you. My approach, and I think the approach from a civil liberties or even just kind of a basic human perspective, is innocent until proven guilty, right? We shouldn't be all treated as if we were suspects. We should be treated as if we are free people. And only if they have evidence should they be empowered to then come and get information about us. And in terms of some of the security measures that law enforcement is hostile to, they actually keep us safe from bad guys too. So in some ways they want us to be less secure in order to make sure their jobs are easier, which I think is just the wrong trade off. So law enforcement in the US has been a leader in this, and now there are others as well.

Andrea Chalupa (14:38):

In terms of what harm this can cause people; if you're an activist… Let's say you're a dissident from an authoritarian regime. What are some ways that this could really mess with your life, this constant surveillance?

Cindy Cohn (14:53):

Well, EFF represents a woman, a Saudi Arabian activist, who is one of the women who's been driving, right? Who's been going and, and driving cars. Her name is Lujan. She had spyware put on her phone via Apple, via an update that ended up getting her found when she was in hiding and arrested and tortured in Saudi Arabian jail. She's out now and she has asylum, but we're talking about life and death. We're talking about the lack of security and kind of end-to-end built in protections in our technology and the surveillance business models that literally take people's lives. Now, the targeted malware business model isn't the same as the mass surveillance business model, but they kind of all work off the same idea, which is these devices we have leak data, leak information about us.

Cindy Cohn (15:46):

And sometimes that's deliberate, and sometimes it's not deliberate. But either way, they can be a vector towards really, you know, old school direct human rights abuses like disappearances, torture, improper arrest. For other people who aren't, say, dissidents dealing directly with an authoritarian, the impacts are difficult to trace but they're real, right? The company that decides whether you get a mortgage or not is running analytics on you to try to decide whether you get a mortgage or not. If those analytics are not good, you may not get a mortgage or you may get it at a higher rate. You might not be able to get a student loan. And again, we have also worked with people who have far more direct impacts; people who, again, are dealing with child protective services who've had their kids taken away because an algorithm predicts that they're not a very good parent.

Cindy Cohn (16:38):

In the context of facial recognition, we've seen a number of false arrests, almost always of African American men who are falsely identified in facial recognition systems. We've seen those same facial recognition systems being used by, say, Madison Square Garden to deny access to events to a list of, you know, basically a blacklist that the Madison Square Garden Company has put together of people who've sued them or have otherwise they don't like. And so facial recognition is being used to deny people access to public accommodations. I mean, it's hard to kind of put your head around all of it and have an easy story to tell, but there's a reason that privacy is a human right. We all wanna have privacy, we all wanna have security, and we all want fair dealing. But when these companies and governments have asymmetric access to information about us that they're using to make decisions about us, then it's not fair.

Andrea Chalupa (17:38):

What about a name that comes up a lot in terms of the movement across America to try to bring far-right candidates to power, and that is Peter Thiel. He's a libertarian of Silicon Valley that we often reference on the show, and he has his Palantir technologies. Is he somebody who you've been following? What concerns and red flags do you see with Peter Thiel generally with his work in regards to all this?

Cindy Cohn (18:06):

I mean, I wouldn't call myself a Thiel expert but I've met Peter and watched the things he's done. I think that you start with a severe hostility to a free press, right? And the funding of the lawsuit against Gawker Media that he did to basically bankrupt a journalistic entity that had embarrassed him. I think that's a very dangerous tendency and, you know, that rich people shouldn't be able to basically bankrupt the news because they don't like what the news is doing. I think that Palantir is a company that EFF is long criticized for, you know, basically selling surveillance capabilities to ICE, to law enforcement and, you know, kind of overpromising what they can deliver but still it's very problematic. To build a system that is named after a bad guy, but that really tries to supercharge government surveillance.

Cindy Cohn (19:04):

So I think it is problematic and I wish Peter Thiel would turn his energy towards something better than his own petty grievances and spying on all the rest of us because there's so many things that could use help like this. But I actually think our bigger goal ought to be to get away from the world in which we have all these dictators, right? The answer to a bad dictator is not a better dictator. The answer is to get rid of the dictators. And I think that a world in which we're all focused on these really rich guys and their picadillos and the things that they do or don't do is always somewhat broken, right? Even if they were the best people in the world—and they're definitely not—it's still not the right model. The model is we need to grab control back of these things.

Cindy Cohn (19:53):

We need to reintroduce competition and have a range of places that we can go and have our conversations and do our organizing and make our political actions there. I'm a big fan of some of the stuff that's happening in the Fediverse to try to re-decentralize the internet. And part of the reason to do that is a lot of the free speech and privacy problems we have are a side effect of the centralization and the surveillance business model. But also I just think it's a lot easier to govern smaller spaces and they give users like you and me a lot more options to pick the places we wanna be and leave the places we don't wanna be at anymore, which is something that ought to be easy for people to do and right now is quite hard.

Andrea Chalupa (20:40):

Where are you spending your time on social media? Where do you feel that it's safe and you can engage with the community and you have relative peace of mind?

Cindy Cohn (20:50):

I mean, I don't engage very much. I admit that I'm a privacy activist because I'm really a big fan of privacy, so I'm not somebody who engages personally on social media a lot. But EFF certainly does and we try to be all the places where people are. I would say that right now, you know, I made the shift to Mastodon quite a while ago and that's certainly growing a place where I get my news and information and is just a gentler place than Twitter has been. But I might not be the best model for this. Again, I'm not a big social media person. I believe that it's really great that digital technologies have enabled people to live their lives in public if they want to, but I think it also needs to make it available for those of us who don't want to.

Andrea Chalupa (21:34):

And what are some ways to protect ourselves online from surveillance? You mentioned staying off of social media. What are some other ways? Is it just like, don't go online?

Cindy Cohn (21:45):

Well, no, I think that's really sad and I wouldn't want that to be the answer. In fact, I think that the most important thing for people to do if they want a better online experience, honestly, is to join with EFF and a bunch of other organizations to make their voices heard about changing some of the laws and the policies surrounding our world because there are not a lot of good choices, right? You know, I also don't think that we should all just go live in a cave and not use technology. I love technology. I work for the Electronic Frontier Foundation. We believe in the benefits of technology. And so we have to stand together to try to make sure we get those benefits and we stomp out the bad things. And some of that's gonna mean we need comprehensive privacy law.

Cindy Cohn (22:23):

It means that we need to do some things in the way our law and policy works that are different. We need to reinvigorate antitrust law and competition law. We need to make sure that the rules that are getting in the way of people starting up competitors right now get out of the way because there's tons of people who have tons of good ideas about what they wanna do. But right now, the world is set up so that you gotta go on bended knee to one of the oligarchs and ask them for, you know, either the money or the permission or the model to go forward. And again, this is why I am excited about the Fediverse and the opportunities that a protocol like Activity Pub and Mastodon make possible for people to be able to not only find better communities, but leave communities when they get toxic and start new ones.

Cindy Cohn (23:13):

And I think that's just the way toward a better world. Now, what can you do if you're somebody who's facing, you know, direct repression like the activist that you referenced, or a journalist? Well, EFF has a set of tools called Surveillance Self-defense (SSD) that will walk people through their particular threat models and what kind of options they might have to try to protect themselves better. We just launched a new one that’s aimed at reproductive justice, so people who are seeking an abortion or seeking to help people with abortions, we have a set of things you can do to try to reduce the risk. We can't eliminate it, but reduce the risk that that community is facing. We even have a set of tools called the Security Education Companion, which are tools for people who want to be trainers, who wanna help other people develop the skills that they have, a kind of pedagogically useful tool, so that if you're somebody with tech skills and you wanna use those skills to try to help make other people safe, these are some ways to help you learn how to be a good teacher.

Cindy Cohn (24:14):

We do direct assistance. We help people all over the world who need direct assistance. But I think for people who aren't in the spotlight like that, one of the things they ought to put on their list to do, in addition to, you know, downloading Signal and using Tor when they need to, is actually joining with the organizations that are fighting to make a better world because some of these things we can't solve through individual choices.

Andrea Chalupa (24:36):

And where can people find those toolboxes that you mentioned? The EFF website?

Cindy Cohn (24:42):

Yeah, the EEF website. It's ssd.eff.org for Surveillance Self Defense. But if you go to our main page and just type in those things, you'll get to them pretty fast. There are other toolkits that other organizations have put together too. Sometimes we work with them. Ours isn't the only one, but it is relied upon by a lot of people around the world and we try to keep it updated. AndI think it's a useful exercise for people to do this. We use a technique that is called threat modeling, right? You actually need to think about who you are and what your threats are so that you can set things right, because the things that my protected journalist against, you know, the Chinese government might not be the same things that a reproductive justice activist needs to do.

Cindy Cohn (25:26):

And so thinking about this from the perspective of who you are and what your threats are is really important to getting it right, and also to not getting overwhelmed with all of the choices. At the end of the day, you can't solve this with personal choices. We need to address the surveillance business model. We need to address law enforcement's increasing interest in making sure that we don't have very secure tools, and companies who want to sell us out. We need to address those things directly and collectively, not just individually.

Andrea Chalupa (25:58):

Absolutely. What are some ways that algorithms are wreaking havoc and does that fall into your work?

Cindy Cohn (26:05):

It does a little. I guess I think about it a little differently. I mean, algorithms are… It's a general term for just a set of instructions, right? A recipe is an algorithm, you know? I just did an algorithm and made deviled eggs this morning. I think what you're referring to is the kind of issues around, you know, how the algorithms that are in, say, our social media feeds might be leading to destructive information getting better play than it would otherwise get. I think overall we're in this age of artificial intelligence and machine learning where we need to figure out how to have accountability and due process around the use of these tools. And that's particularly hard in the context of machine learning because it is difficult even for the people running the system to know why it's doing the things it's doing.

Cindy Cohn (26:59):

There's a lot of work being done to try to bring transparency and accountability in that area and EFF is definitely supportive of that. I think that the problem is a little trickier than just “the algorithm is a problem" kind of framing sometimes we see in popular culture, but it doesn't mean it's not worthy of being addressed. Sorry, that was a bit of a dancey answer, but I think that one of the things that's problematic is Twitter has dismantled its algorithmic accountability team. We're seeing things moving away from algorithmic accountability. I think we're seeing this as well with some of the layoffs at Meta and other places where you see these kinds of accountability efforts really weren't very supported to begin with and now being less funded as the companies are retrenching a little bit.

Cindy Cohn (27:47):

And so I think it's really important to keep the energy on around transparency and accountability. There's a couple of proposed federal laws around this that I think could be very helpful. I don't buy the, "We are all just puppets" theory of this; that people don't have free will or agency and whatever the algorithm shows them is what they're all independently gonna believe. I don't think the actual hard scientific analysis has really supported that and I think we need to think about how to bring accountability and transparency into algorithmic decision-making from a place of science and really understanding what it's doing and what it's not doing.

Andrea Chalupa (28:28):

So the big shocking headline we had in recent years was that Instagram was pushing algorithms that turned out to be harmful, causing young girls to self harm. That obviously hasn't really been met with much of a correction, it sounds like. But what about families of somebody that's harmed themselves on account of the reporting on the Instagram algorithms driving young girls, according to that reporting, to self-harm? What are the liabilities there? Can those families sue? Can those girls sue? Can these social media companies be held accountable?

Cindy Cohn (29:02):

Well, we have two Supreme Court cases right now that are under consideration, one of which is testing this theory. I wanna be clear: I really appreciate the work that Frances Haugen did and other people to get this information out of Meta. It did come out that like 1/3 of girls reacted negatively 2/3 of girls reacted positively, I believe. Now, 1/3 of girls is not good and we definitely need to think about how to address that, but I think it's, again, important to be more clear-eyed than sometimes I see in terms of what the data is showing. And that's Facebook's internal, you know, Meta/Instagram's internal data. Again, I think it's important to continue to hold these companies' feet to the fire about, you know, what is it your algorithm is doing and do you know? Because most of the time they have internal studies where they're watching this kind of thing and then to hold themselves to do the things that they're supposed to do. And so Meta disabling its internal accountability teams and shifting them around and all of that is very, very problematic. So I think we need to continue to hold their feet to the fire. We are going to see in the Supreme Court decision, in the Taamneh case coming out in June—I don't know when this is gonna run—but the argument that Twitter should be held responsible because of ISIS content that was available on Twitter and that they weren't able to take it down in time, or they didn't try, or whatever you wanna do. Now, this is the argument that Twitter should be held responsible for the results of a bombing that happened because it allowed ISIS content on its platform.

Cindy Cohn (30:37):

So we'll see what the Supreme Court does on that, but I'm very nervous about holding platforms accountable for later actions that other people take. And the argument that it was as a result of what somebody saw, to me, needs a very, very high bar of proof before I would do it. And the reason for that is we hear this argument all the time being used to try to censor all sorts of things, right? You know, we're in a time right now where we have states in the United States that wanna censor information about trans kids, about the civil rights era, about our culture because it might harm kids and it's causing kids to have harm. So this argument is really important that we are very clear-eyed about when we're using it, what we're using it about, and the evidence to support it.

Cindy Cohn (31:25):

Because once we do it for one reason, you know, “Who will think of the kids?” is a time-honored way that we see a lot of things that we otherwise care about being subjected to actual direct censorship. So I get a little nervous around some of those arguments. It doesn't mean that we can't hold their feet to the fire, but creating liability for a platform because a kid sees something that their parents or that the broader society doesn't want them to see is, to me, the kind of argument that leads to censoring off information around LBGT, around trans rights, around reproductive issues, around all sorts of other things that I think people have to recognize that your arguments… they're not just gonna be used by people you agree with.

Andrea Chalupa (32:12):

Where do you see AI fitting into everything?

Cindy Cohn (32:15):

I think that artificial intelligence systems need to be carefully monitored so that the people who are impacted by the decision-making have a role in understanding how it works and getting redress if it doesn't work. And the things I'm thinking about are things like predictive policing, right? There are systems that are sold—I think the name has changed a bunch of times—that basically try to predict where crime happens. If you look at what's going on there, it's looking at what police do and then trying to say that crime is gonna happen based on where police think there's gonna be crime. Well, we know police only find about half the amount of crime and that they over-police certain neighborhoods and under-police other neighborhoods. So if you're using an artificial intelligence or machine learning algorithm and you're feeding it in what the cops do, it's gonna double down on the racism that we already see in so many police activities across the country.

Cindy Cohn (33:15):

So you have to really look at what are you using artificial intelligence for and who's being impacted on it, and what are you training it for? There's just a range of really important questions before we use AI systems to try to predict people's behavior or to try to do things that are gonna limit people. Now, the techniques themselves are interesting and you can do some cool things with them. You know, artificial intelligence has, I think, great promise in a lot of things around medicine where trying to figure out the patterns in a big chunk of behavior or a big chunk of data, it does better than humans do. And there's a lot of data that we could benefit from using those kinds of tools. So I think of AI as a tool. I think where AI goes wrong is when it's being used, first of all, to try to predict things where we don't know the ground truth.

Cindy Cohn (34:09):

Google is pretty good at predicting whether you wanna buy shoes or not, but that's because it knows at the end of the day whether you bought shoes. Trying to predict whether somebody's gonna be a criminal or not, or worse yet a terrorist or not… We don't have ground truth about future activities like that, such that we can train up a model. But I think it's really important to pay attention to; where are we using AI? What for? What's the benefit? What are we training it for and what is it solving it for? And that's a much harder set of things to do, but it'll take us to a better set of answers about where using these massive models is helpful and where it's not.

Andrea Chalupa (34:48):

There seems to be anxiety about this coming AI age; that it's going to—like social media—fall into the wrong hands, as we've seen with what Musk has been doing with Twitter. Do you feel that? I know you're on the front lines of trying to build collective action for accountability and protections, but do you get a sense that AI will be making everything worse, more polarization, more online harassment by bots, more censorship, more oligarchs like Musk and Thiel disrupting community, do you think it's sort of, Wow, this is it, here comes *The Matrix*?

Cindy Cohn (35:24):

I don't. It's a huge jump in the way technology works and the things that it can do, and every single one of those has good things and bad things in it. I think if we want to reduce the bad things, we have to pay attention now. We can't just stick our heads in the sand and we can't just decide that we don't want any of it because I don't think that's gonna happen. There are tons of good uses for the big language models and things like that. If we had a world in which we actually took care of people when they lost their jobs, there are a lot of jobs that could be replaced by technology and that would be a good thing. AOC says, "Look, I'm not in favor of keeping people in shitty jobs because of fear of automation."

Cindy Cohn (36:08):

What what we need to do is we need to get better at making sure that we help people whose jobs might be eliminated actually have a landing pad and have other things to do and have universal basic income and other things, rather than trying to stop the use of technology to automate jobs that otherwise are not all that great for people. So I think that's one of the things we need to do. I just don't think we can be all or nothing about AI. I don't think that's particularly realistic, even if we took that position. I think we need to do the hard work of figuring out; how can this technology go wrong? Where can it go wrong? How can we mitigate those things? And how can we as a society help make sure that we're supporting the people who are facing those issues? And luckily, there's quite a lot of work being done right now, but you know, we're not pulling the levers of power just yet and we're gonna need to get to the place where we can do that too.

Andrea Chalupa (37:02):

What about private surveillance groups like Black Cube and how they're increasingly tech disruptive/tech savvy when they have a target, as Ronan Farrow has shared in his book, *Catch and Kill*? Are groups like Black Cube on your radar? Is that something that you guys are tracking?

Cindy Cohn (37:22):

Oh yeah, absolutely. And in fact, you know, I told you the story of the Saudi Arabian woman who was tortured and that company is called Dark Matter. They all have these, you know, cloak and dagger names I guess. But yes, EFF is part of a wide range of groups around the world who are tracking this, who are trying to deal with these companies that get employed by governments, often, to do this kind of work. There's a program called Pegasus that our friends at Citizen Lab have investigated that's being used all across Mexico to track and has been linked to disappearances and murders of journalists and activists down there. So yes, this is something that we track a lot. We try to help people get some of the tools they need to protect themselves. As I said, we tried to bring a lawsuit in the United States to hold Dark Matter accountable for basically disguising itself as an Apple update in order to attack our client's phone.

Cindy Cohn (38:16):

And, you know, we lost at the district court level. We're going up in the court of appeals. We brought an earlier case a few years ago on behalf of an Ethiopian activist who also had his computer attacked by the Ethiopian government in Washington DC where he was living. The case was called *Kidane*. And sadly, the courts just were not willing to recognize that foreign governments were engaging in this kind of behavior against Americans in America. But we need to change that because, you know, we need to be able to bring the tools of accountability to bear on this kind of horrible, horrible behavior.

Andrea Chalupa (38:51):

And that brings us to Russia. Have you been helping any dissidents from Russia and Ukraine in regards to Russia's far reach through their well-known cyber capabilities?

Cindy Cohn (39:01):

You know, I think that some focus on the EFF team have been helping, but there is a wealth of organizations that are doing that as well. I mean, on the one hand, you know, Russia has very powerful spying capabilities. On the other hand, a lot of the Ukrainians do too. So this is a situation in which there are pretty high tech skills on all sides of the debate. So we help people where we can and there's a lot of other groups that are helping people as well. But it's a different kind of situation than some of the other ones because, again, it's not like the Ukrainians didn't have a sophisticated tech sector themselves.

Andrea Chalupa (39:38):

What about the border; surveilling the border and the horrible human rights abuses that have been carried out on our southern border for a while now but certainly in the last several years and a lot of horrible high profile cases? Are you seeing advancements there in terms of how the border patrols there are relying on this sort of dystopian tech? What is coming out of that?

Cindy Cohn (40:00):

Yeah, no, in fact, EFF has a project called the Atlas of Surveillance where we are trying to identify and track all of the surveillance that is happening across the United States by various kinds of law enforcement. And we have just completed three trips to the border, specifically to try to identify and monitor and help organize around specifically surveillance at the US/Mexico border, the southern border. And so we do a lot of work in trying to give people the tools they need to see and identify the surveillance that's happening to them. EFF also worked with the ACLU to try to… We brought some litigation to try to argue that the 4th Amendment should attach at the border, which stops the kind of suspicion list search and seizure that happens.

Cindy Cohn (40:54):

We did not succeed in that case, but we're looking for another one because we think, you know, your rights shouldn't stop at the border and law enforcement and the border patrol folks ought to abide by your constitutional rights even when you're at the border. So it's an ongoing work, and we do a lot of work in this area. You know, it's sad because the Biden administration really has embraced this idea of a digital wall rather than the physical wall that the Trump administration had. And it's extremely problematic. It's not a good idea. I don't think it's a better idea than the physical wall was, which was a horrible idea. So I think that this is an area where I think the Biden administration is really on the wrong foot and it's important that not, you know… I mean, the first step in this is that, you know, people don't even know all the surveillance equipment that is installed right near their homes that they could be subject to.

Cindy Cohn (41:44):

So the Atlas of Surveillance is the first step to try to get attention to this and then to try to get. There are some ordinances that EFF has helped pass in various places, including here in Oakland, California and some other places, where if law enforcement wants to adopt new surveillance technologies that would impact people, they have to go through a public process and get public approval to do it. And those ordinances just passed in a few places, but they're an extraordinary tool for local people to really begin to get their hands around what surveillance is actually being deployed directly aimed at them.

Andrea Chalupa (42:22):

Great. And that's something that local governments anywhere in the country could adopt.

Cindy Cohn (42:25):

Absolutely. It's a real problem. A lot of places in this country—and I think this is a shock to people—there isn't much local control over what tools the cops get. And sometimes that's the sheriff, sometimes that's the cops, sometimes they get a lot of surplus military equipment. All of these things should all be subject to local control, right? You should be able to say, Look, my local cops shouldn't have a stingray. My local cops shouldn't be able to have a tank, right? Without the community saying that's okay. But these ordinances—CCOPS is what the shorthand for them—is to try to make sure that there's citizen control over the tools that local law enforcement have. So this is something people, we have a group called the Electronic Frontiers Alliance that is local groups all across the country that organize around local community issues and trying to get these ordinances passed in various places across the country is some of the work that some of those groups have done.

Andrea Chalupa (43:21):

What do you envision as the ideal future of the internet and how could we build that?

Cindy Cohn (43:26):

Oh, this is such a good question. In fact, we started a podcast at EFF called *How to Fix the Internet* in order to really try to address this. I feel like we can't build a better internet unless we can envision it, and so many of us have really lost the ability to imagine something better than this, you know, kind of somewhat lousy technical world that we have right now. And I think we're all kind of circling the drain around the possibility that digital tech could do anything other than make our lives worse. So we started the podcast, *How to Fix the Internet*, in order to kind of force ourselves but also bring in people who are envisioning a better world so that we can have a shared idea of where we're headed. So thank you so much for asking that question.

Cindy Cohn (44:10):

You know, sometimes as a civil liberties lawyer, you spend all your time going, “This is horrible and this is horrible and here's why this is bad,” and so putting on a different hat is really important. So, what are the things that I think have come up as part of a better world? Well, first of all, your tools answer to you and you alone, and the people that give you tools and services have a duty of loyalty to you, just like your lawyer has a duty of loyalty to you, or your accountant has a duty of loyalty to you. You go to your accountant to do your books, you don't have to worry that they're secondarily selling your information to somebody who might wanna, you know, sell you a copy of Intuit, right? That's not the way it should work in an accounting relationship.

Cindy Cohn (44:52):

And that's the way it should work for most of your online services and tools; that they should have a duty to you, they just serve you and you have control over how things work. You have the ability to leave. If you don't like a service and it's not working for you, you have the ability to leave and take your data and your connections and the other things that you built there with you. It's a pretty simple idea. What else? I would love to see technologies that fit our bodies better. I think a better world would be one where we don't have this neck where we're looking down all the time at our systems. So I think we should think even more broadly than civil liberties about what kind of technical world we want to build. I think a better world will have security end-to-end built into most of the stuff that we do, will have accountability and transparency so that when things go wrong—because they always do—we will know that things have gone wrong and we will have a way to have personal accountability for those problems; if there's a data breach or something like that.

Cindy Cohn (45:51):

And then I also think that it's a world in which we have a lot more choices about the communities and you know, on the social networking side that we can have communities that serve us and if they're not serving us, we take our data and leave and go start another one. And that the barriers to that ought to be much, much lower. So those are some of the things that have come up in the conversations that we've had that I think are really important to building a better, more secure world where, you know, people can speak their minds and begin to build movements and community building online. And if that starts to turn toxic, everybody can leave and that little world will die. We're not headed there right now, you know? Instead we've got a crazy manchild dictator deciding what should happen on what used to be the place where a lot of people got their news and community, and I think that envisioning a world in which more of us have more control is a start.

Andrea Chalupa (46:47):

Wonderful. Thank you so much Cindy Cohen. Appreciate it. Appreciate all the work you do and thank you for that really rich conversation.

Cindy Cohn (46:54):

Oh, thank you very much. Thank you for your really smart questions.

[outro theme music, roll credits]

Andrea Chalupa

Our discussion continues and you can get access to that by signing up on our Patreon at the Truth-teller level or higher.

Sarah Kendzior:

We encourage you to donate to help rescue and recovery efforts in Turkey and Syria following the devastating earthquakes in early February. To help people in Turkey, visit the TPF Turkeye Earthquake Relief fund at tpfund.org

Andrea Chalupa:

To help Syrians in need donate to the White Helmets at whitehelmets.org. We also encourage you to help support Ukraine by donating to Razom for Ukraine at razomforukraine.org. In addition, we encourage you to donate to the International Rescue Committee, a humanitarian relief organization helping refugees from Ukraine, Syria, and Afghanistan. Donate at Rescue.Org. And if you want to help critically endangered orangutans already under pressure from the palm oil industry, donate to the Orangutan Project at theorangutanproject.org and avoid products with palm oil.

Gaslit Nation is produced by Sarah Kendzior and Andrea Chalupa. If you like what we do, leave us a review on iTunes. It helps us reach more listeners and check out our Patreon. It keeps us going.

Sarah Kendzio:

Our production manager is Nicholas Torres and our associate producer is Karlyn Daigle. Our episodes are edited by Nicholas Torres and our Patreon-exclusive content is edited by Karlyn Daigle

Andrea Chalupa:

Original music in *Gaslit Nation* is produced by David Whitehead, Martin Visseberg, Nik Farr, Demien Arriaga, and Karlyn Daigle.

Sarah Kendzior:

Our logo design was donated to us by Hamish Smyth of the New York-based firm, Order. Thank you so much, Hamish.

Andrea Chalupa:

Gaslit Nation would like to thank our supporters at the Producer level on Patreon and higher with the help of Judge Lackey, the narrator of the new Gaslit Nation graphic novel, *Dictatorship: It's Easier Than You Think…*