Podcast Episode: The Secret Court Approving Secret Surveillance

November 12, 2020

Rainey Reitman

Episode 001 of EFF's *How to Fix the Internet*

Julian Sanchez joins EFF hosts Cindy Cohn and Danny O'Brien as they delve into the problems with the Foreign Intelligence Surveillance Court, also known as the FISC or the FISA Court. Sanchez explains how the FISA Court signs off on surveillance of huge swaths of our digital lives, and how the format and structure of the FISA Court is inherently flawed.

In this episode, you'll learn about:

- How the FISA Court impacts your digital privacy.
- The makeup of the FISA Court and how judges are chosen;
- How almost all of the key decisions about the legality of America's mass Internet spying projects have been made by the FISC;
- How the current system promotes ideological hegemony within the FISA court;
- How the FISC's endless-secrecy-by-default system insulates it from the ecosystem of jurisprudence that could act as a guardrail against poor decisions as well as accountability for them;
- How the FISC's remit has ballooned from approving individual surveillance orders to signing off on broad programmatic types of surveillance;
- Why we need a stronger amicus role in the FISC, and especially a bigger role for technical experts to advise the court;
- Specific reforms that could be enacted to address these systemic issues and ensure a more fair review of surveillance systems.

Julian is a senior fellow at the Cato Institute and studies issues at the intersection of technology, privacy, and civil liberties, with a particular focus on national security and intelligence surveillance. Before joining Cato, Julian served as the Washington editor for the technology

news site *Ars Technica*, where he covered surveillance, intellectual property, and telecom policy. He has also worked as a writer for *The Economist*'s blog *Democracy in America* and as an editor for *Reason* magazine, where he remains a contributing editor. Sanchez has written on privacy and technology for a wide array of national publications, ranging from the *National Review* to *The Nation*, and is a founding editor of the policy blog *Just Security*. He studied philosophy and political science at New York University. Find him on Twitter at @Normative.

Below, you'll find legal resources – including links to important cases, books, and briefs discussed in the podcast – as well a full transcript of the audio.

Please subscribe to How to Fix the Internet using Stitcher, TuneIn, Apple Podcasts, Spotify, or your podcast player of choice. You can also find this episode on the Internet Archive. If you have any feedback on this episode, please email podcast@eff.org

Resources

NSA & FBI

- Stellar wind
    - NSA Collected US Email Records in Bulk for More than Two Years Under Obama (The Guardian)
    - NSA's Stellar Wind Program Was Almost Completely Useless, Hidden From FISA Court by NSA and FBI (Techdirt)
- FAQ on NSA surveillance, including FAQs about EFF's litigation to stop the mass surveillance (EFF)
- Pen trap and trace authority and wiretap authority and other electronic surveillance, including Title 3 (relevant to wiretaps)
- Crossfire Hurricane
    - Crossfire Hurricane (Wikipedia)
    - Read the Inspector General's Report on the Russia Investigation (New York Times)
- Carter Page: Justice Department Says Facts Did Not Justify Continued Wiretap of Trump Aide (New York Times)

Court Cases

- Smith v Maryland (Wikipedia)
- Smith v Maryland Turns 35, But Its Health is Declining (EFF)
- US v. Miller (Wikipedia)
- U.S. v. Maolin Ninth Circuit Opinion (ACLU)

- United States v. Maolin case page and brief (Brennan Center)
- United States v. Maolin case page (EPIC)
- Jewel v. NSA case page (EFF)
- About Federal Judges - Article III Judges (US Courts)

Section 215 & FISA

- What You Need to Know about the FISA Court- and How it Needs to Change (EFF)
- FISA Court Docket
- Foreign Intelligence Surveillance Act
- Reform or Expire (Section 215 of the Patriot Act) (EFF)
- Enhancing Civil Liberties Protections in Surveillance Law (2015 USA Freedom Act and the introduction of amici) (Brennan Center)
- Classified Information Procedures Act (CIPA) (Wikipedia)
- The Classified Information Procedures Act: What It Means and How It's Applied (Lawfare)

Books

- Code and Other Laws of Cyberspace 2.0 by Lawrence Lessig
- National Security Investigations and Prosecutions by Douglas Wilson and David Kris

Transcript of Episode 001: The Secret Court Approving Secret Surveillance

Danny O'Brien:
Welcome to How to Fix the Internet with the Electronic Frontier Foundation, a podcast that explores some of the biggest problems with face online right now. Problems whose source and solution is often buried in the obscure twists of technological development, societal change, and subtle details of Internet law.

Cindy Cohn:
Hi everyone, I'm Cindy Cohn, the Executive Director of the Electronic Frontier Foundation, and I'm also a lawyer.

Danny O'Brien:
And I'm Danny O'Brien, and they let me work at EFF too—even though I'm not a lawyer. Welcome to How to Fix the Internet, a podcast that explores some of the more pressing problems facing the net today and then solves them. You're welcome, Internet.

Cindy Cohn:
It's easy to see everything that's wrong with the Internet and the policies that govern it. It's a lot harder to start naming the solutions to those problems, and even harder sometimes to imagine

what the world would look like if we got it right. But frankly, that's the most important thing. We can only build a better Internet if we can envision it.

Danny O'Brien:
So with an ambitious name like 'How to Fix the Internet', you might think we're going to tackle just about everything. But we're not, and we're doing that on purpose. Instead, we've chosen to go deep on just a few specific issues in this podcast.

Cindy Cohn:
And sometimes we know the right answer—we're EFF after all. But other times, we don't. And like all complex things, the right answer might be a mix of different ideas or there may be many solutions that could work or many roads to get us there. There is also some bad ideas some times and we have to watch for the blow back from those. But what we hope to create here is a place where experts can both tell us what's wrong, but give us hope in their view of what it's going to look like if we get it right.

Danny O'Brien:
I do feel that some parts of the digital world are a little bit more obviously broken than others. Mass surveillance seems like one of those really blatant flaws at EFF we've spent years fighting pervasive US government surveillance online and our biggest fights have been in what seem to us the most obvious place to fight it, which is in the public US courts. But there is one court where our lawyers will likely never get a chance to stand up and argue their case. Even though it's got surveillance in its name.

Cindy Cohn:
Our topic today is the Foreign Intelligence Surveillance Court, which is also called the FISC or the FISA Court. The judges who sit on this court are hand picked by the chief justice of the United States Supreme Court, that's currently Justice Roberts. The FISA Court meets in secret and has a limited public docket and until recently it had almost no public records of its decisions. In fact, the very first case on the FISC docket was an EFF transparency case that ended up getting referred to the FISC. But this where almost all of the key decisions about the legality about America's mass Internet spying projects have been made and what that means is pretty much everybody in the United States is affected by the secret court's decisions despite having no influence over it and no input into it and no way to hold the court accountable if it gets things wrong.

Danny O'Brien:
Joining us now to discuss just what an anomaly an American and global injustice the secret FISA Court is, and how we could do better is Julian Sanchez, the Cato Institute's specialist in surveillance legal policy. Before joining Cato, Julian served as the Washington editor for Ars Technica where he covered surveillance, intellectual property and telecom policy. He has also worked as a writer for the Economist blog, Democracy in America and is an editor for Reason Magazine where he remains a contributing editor. He's also on Twitter as Normative and that's one of my favorite follow there.

Danny O'Brien:
Julian, welcome to the podcast. We are so happy to have you hear today.

Julian Sanchez:
Thanks for having me on.

Cindy Cohn:
Julian, you have been incredibly passionate about reining in mass surveillance for as long as almost anyone, perhaps even me. Where does that passion come from for you?

Julian Sanchez:
I don't know if I have an origin story. I was bitten by a radioactive J. Edgar Hoover or something, but as an adolescent I was in a way much more technical than I am now. I ran a dial-up BBS when that was still a thing before everyone was on the Internet and I remember watching people dial in and I think it was something people sensed was a private activity as they were writing messages to each other and tooling around looking for things to download. Sometimes I would just be sitting there watching them and thinking, gosh, the person who operates the platform really has visibility on a lot of things that we don't instinctively think of as observed. Probably just as a result of being online, for some values of online from a pretty young age, I was interested in a lot of the puzzles of how you apply rules that we expect to govern our conduct in the physical space to this novel regime.

Julian Sanchez:
I remember in college jumping ahead and reading Lawrence Lessig code and discussing the puzzle of the idea of a perfect search. That is to say, if you had a piece of software, a virus let's say, that could go out and look only for contraband, it would only ever report back to the server if it found known child pornography or known stolen documents. Would that constitute a search? Is that the kind of conduct that essentially, because it would never reveal anything but contraband, could be done universally without a warrant or should we think differently about it than, for example, the Supreme Court thinks about dog sniffs. If it only ever reveals what is criminal, that is, the presence of narcotics or bombs, then it doesn't technically count as a search even though it is a way of peering into a protected space.

Julian Sanchez:
more recently, whimsically, the Risen and Lichtblau story back in 2005 'Bush Lets US Spy on Callers Without Courts,' which was the first public hint of what we later came to know was a mass program of warrantless surveillance called, Stellar Wind. I was just dissatisfied with the quality of the coverage and ended up buying the one book you could get about FISA, 'National Security Investigations and Prosecutions' by David Kris and Douglas Wilson, and burning through it like Harry Potter. I just found it inherently fascinating. This was at a time when, and I was still a journalist at the time, it was a time when most of the reporters writing about this did not understand FISA very well. They certainly had not read this rather thick, and to normal human beings, boring treatise and so I found myself, because I now have this rather strange knowledge base, writing quite a lot about it, partly just because the quality of a lot of the coverage of the issue was not very well informed.

Cindy Cohn:
We had a similar experience here at EFF, which was, at that time it was my colleague, Lee Tien and I, and we had read Kris and so we ended up becoming the only people around who knew about the secret court before everybody suddenly became aware of it. But let's back up a second. Why do we have a FISA Court? Where is it? I've talked a little about who is on it, but where does this idea come from?

Julian Sanchez:
This grows out of the Foreign Intelligence Surveillance Act of 1978 that was passed in response to disclosures of a dizzying array of abuses of surveillance authority and their power more generally by the FBI especially, but the American intelligence community in general. For decades, oversimplifying a bit, effectively wire tapping had been initially just illegal period and then very tightly constrained and the FBI had essentially decided those rules can't possibly really apply to us and so FISA, for the first time, created an intelligence specific framework for doing electronic surveillance. The idea of having a separate court for this, I think, grew out of a number of factors.

Julian Sanchez:
One is the sense that there was this need for extreme secrecy where you were dealing with potentially people with foreign state backing who were not necessarily going to be sticking around for criminal prosecution. And when you're talking about intelligence gathering, criminal prosecution isn't necessarily the point. And so this is an activity that is not really designed to yield criminal cases. You don't really want the methods ever disclosed. You're dealing with adversaries who have the capability to potentially plant people in ordinary courts, that's where you're discussing interests, sources, and methods in your intelligence so there was a sense that it would be better to have a separate, extra secure court. And also that you might not want to have to explain all this both highly sensitive and potentially quite complicated intelligence practices and information to whatever random magistrate judge happened to be on the roster in the jurisdiction where you were looking.

Julian Sanchez:
And also that the nature of intelligence surveillance is quite different in so far as, again, you're not necessarily looking at someone who has committed a crime, you think someone is working on behalf of a foreign power and trying to gather intelligence for them or engage in clandestine intelligence activities. But you don't necessarily have a specific crime you think has been committed. Your purpose in gathering intelligence is not to prosecute crimes. These are the cluster of reasons around the formation of a separate court for that purpose and it originally consisted of seven federal circuit judges, now it's 11 after the USA Patriot Act increased the number and so they continue serving on their regular courts and then, in effect, take turns in rotation sitting for a week and hearing applications from the Justice Department and the FBI to conduct electronic surveillance.

Cindy Cohn:
The court started out as one thing, this idea of individual secret warrants for spies basically, but

it's really changed in the past decade. Can you walk us through how those shifts happened and why?

Julian Sanchez:
And of course to the extent that older FISA Court opinions are not available. The first ever published opinion of FISA Court was in 2002 and it was quite a few years before we got a second. Now quite a number of more recent ones are public, but we still have to speculate about the earlier history of the court, but veterans of the court, that is retired FISC judges have effectively confirmed that, in its early years the FISA Court was primarily about assessing the adequacy of individual warrant applications. It was just a bread and butter magistrate judge usually almost scut work. Okay, have you made the showing that there is probable cause to believe that the target of the surveillance is an agent of a foreign power. You have, you haven't. In 99.9% of cases, it was, you have and they took a pass on that individual warrant and as we get to the, in particular, the post-9/11 era and you're dealing with questions of trying to, one, often figure out who an unknown target is. You might have someone whose using a particular email address or other account that you don't otherwise necessarily have an identity.

Julian Sanchez:
You're potentially trying to sift through a lot of data to figure out who your target is or which data pertains to the people you're interested in. There is a shift toward more programmatic sorts of surveillance and so the court increasingly is not passing on the question of have you established a probable cause showing with respect to "bad guy X" but rather does the law, does a statute written to deal with pre-Internet communications technology permit you to do the surveillance you're contemplating and in particular, might it allow you to gather information in ways that go beyond just targeting a particular facility, a particular phone line, that is the home phone of a particular known target. And so it ended up building this kind of secret body of precedent around what kinds of programs for Internet type network surveillance were permissible under a statute that was not written with that in mind.

Cindy Cohn:
They really did shift from individual warrants to approving whole programs and whole programs that really went beyond, is this person a spy to let's look at this whole network and see maybe if there is something that indicates that a spy might be there. It really flips the kind of basis way that we think about investigations. From my perspective, obviously, I've been litigating this in the courts for a long time so it kind of flipped the whole thing on its head.

Julian Sanchez:
And so we know, for example, maybe I should give some maybe more concrete examples. We know there was a bulk telephony metadata program under one FISA authority that actually was sort of the second case of this kind the FISA Court had to consider. There was an earlier question presented by a program that used what was called the pen trap authority, pen register trap and trace authority, which is, in the traditional phone context, this is about essentially real-time metadata surveillance. Meaning let's say there's a particular phone number that we think is up to no good, maybe we don't have a full blown probable cause wiretap order for that number yet, but we want to know who this target is calling and whose calling that target.

Julian Sanchez:
A pen register trap and trace order lets you get realtime data about what calls are happening to and from that number and who they are from and how long the call lasts and in the Internet era the question is, what kind of realtime metadata does that let you get and when the statute talks about a facility at which this information collection is directed, traditionally that meant a phone number is the facility, but in the Internet era, you had questions like, because the standard for this kind of trap is because you're not getting full blown, in theory, you're getting the full content, the full email, the full phone conversation. You can get one of these pen trap orders under Section 214 of the USA Patriot Act with a lot less than probable cause.

Julian Sanchez:
The question is, we're talking about regular phones anymore, we're talking about Internet accounts and IP addresses and server. What can a facility be? Can we say, we want all the metadata and the realtime transactional information for a particular server and all the traffic coming to and from that? So we're not just talking about one individual phone line or maybe even a corporate phone line used by a number of people, but facilities that may be handling millions of peoples traffic, or at least tens of thousands of peoples traffic. The court, I don't think that is an opinion that is public in full at this point, but essentially said, at least with respect to international communications, we're going to be pretty permissive about what you can collect.

Danny O'Brien:
This is the other shift that I see, which is that not only is FISA not dealing with regular phones anymore, but it's dealing with these big servers with millions of people, but also the sort of target has changed too, partly because we're not really talking about agents of a foreign power, we're not talking about spy versus spy. It became much more dissolved than that. It's like we're talking about random stochastic terrorists who you don't necessarily know who they are. But also, this switch between "we can do foreign surveillance because we're targeting foreign powers and their spies",to "we're just surveilling foreigners", like they don't have rights under this court. So the question is, how do we scoop out this data and separate the stuff that legally we are concerned about, which is US citizens communications, but everything else is kind of fair game. And then we have a secret court that doesn't even have any kind of representation of US citizens interests, but also making this kind of human rights and foreign policy decision too.

Julian Sanchez:
The debate around the authorities that the FISA Court oversees has been very, US citizens-centric, so you can watch tapes from CSPAN where a lot of defenders are saying, "look, as long as they are targeting foreigners, who cares if they don't have constitutional rights". Some of us think, people are human and have human rights even if they had the poor taste to be born somewhere other than the United States and so this is perhaps not something we should entirely shrug off. But also that there's this interesting shift from the idea that you should be concerned if the communications of an American with Fourth Amendment rights are surveilled too. The idea that really what's significant in terms of encroaching on peoples' rights is who is targeted. And for practical reasons, of course, you understand why this would be the focus because you cannot in advance know whose communications you will intercept when you target somebody. You

know who you're going to target, but you have no idea who they might talk to. That's the point in part of doing the surveillance.

Julian Sanchez:
But if you look at the text of the Fourth Amendment, it doesn't say the "right of the people against being targeted shall not be violated". It says "the right of the people to be secure in their persons and houses" and papers or the digital equivalent thereof. And in a sense, the fundamental Fourth Amendment concern was, at the time, were the general warrants, with the idea of these sort of open-ended authorizations to search, that did not target anyone. From the perspective of the people who signed off on the Fourth Amendment, it was not a mitigating consideration to say, don't worry if your communications are collected, you weren't the target. The thing they found most egregious, the thing they thought was the most defensive abuse was surveillance that did not have a particular target that made it open to anyone to be swept into the dragnet.

Danny O'Brien:
Right. And just to spell this out, general warrants and this is a British invention so I apologize, was this idea that you could just get a warrant for everybody in a town or everybody who might be associated with it so this early mass surveillance warrant.

Julian Sanchez:
And it's intimately connected with political, essentially political dissent and suppression. Some of the most controversial early cases that the American framers looked to involved a publication called the 'North Britain 45', was the one that really annoyed the King and so there was an authorization given to the King's messengers to make diligent search for these unknown anonymous writers and publishers of this seditious publication. The whole problem was it was published in the United States so they didn't know in advance who was responsible so they thought we need the authority to be able to riffle through the possessions of all the folks we suspect of maybe not being as loyal as they ought to be and give them cart blanche to decide who the appropriate targets are so the British courts ultimately said was destructive of liberty in a pretty toxic way. Chief Justice Pratt, later Lord Camden wrote some pretty inspirational prose about why that kind of authority was fundamentally incompatible with a free society and that was a great influence on the defenders of the Fourth Amendment who had the same objection to general warrants or a general search authorizations that empowered customs officials to essentially look for contraband without particularized judicial authorization.

Danny O'Brien:
And there's this subtle thing here where you only get to make that kind of discrimination, that kind of difference particularly when you're separating what is terrorism and what is political action, if there is someone in the court testifying on behalf of the person that might be being targeted and that's what a secret court like the FISA Court just didn't have for a very long time, barely has now.

Julian Sanchez:
Regular courts don't have that either, of course. When you were going to apply for a wiretap, even if it's in a criminal case, you don't call up the lawyer of the person you're wiretapping and

say, would you come in and do an adversarial proceeding in court about whether we can wiretap you. You tend not to get very much useful information that way. But there is the back end, which is to say, yeah, ex parte proceeding on the front end, you don't notify the target in advance that you're going to do a wiretap, but that process is conditioned by the knowledge that the point of a criminal wiretap, a so-called title three wiretap, is to gather evidence for a criminal prosecution that when that prosecution occurs, you're going to have discovery obligations to defense counsel. They are going to have an incentive to kick the tires pretty hard and poke everything with a stick and make sure everything was executed properly and the warrant was obtained properly and if it wasn't, get the case thrown out.

Julian Sanchez:
That knowledge that you've got to expect that kind of wire brush when it comes time to go to court, means that really from the outset, you talk to people who work on getting criminal wiretap orders that they are in consultation with their lawyers and they are talking about how are we going to do this in a way that is going to stand up in court, because if this gets thrown out, you've just wasted your time and probably a fair amount of money in the process. The fact that that doesn't exist on the FISA side, that essentially 99% of FISA orders are not intended to ever result in a criminal prosecution are never going to result in disclosure to target, are effectively, permanently covert means you really don't have to worry about that. You are presenting to the FISA Court your version of "why I think there's evidence that this person is a foreign agent" and if you've cherry picked the facts as seems to have happened in the case of former Trump campaign advisor, Carter Page, if you decided to include the inculpatory information but leave out the information that might call into doubt your theory of the case or make it look like perhaps there's another explanation for some of these things that look incriminating on face.

Julian Sanchez:
You're probably never going to be called into account for that because the FISA Court is relying on your representation and they are probably never going to hear from the target. They put together a very misleading argument for why I was a foreign agent.

Cindy Cohn:
I feel like a part of the problem here is that judges, they really do only get one side of the story. This is one of the reasons that EFF helped get past some changes to the law as part of the USA Freedom Act to create another entity that could at least weigh in and help the court hear from the other side, make it a little more adversarial. But I do think the judges get captured and also one of the things we've learned now is that thanks to the US Supreme Court catching the Department of Justice not even telling criminal defendants when FISA information was used. They are supposed to be telling criminal defendants when FISA information was used and to date, nobody whose been prosecuted even in the public courts on the basis of secret FISA information has ever had access to be able to figure out whether what they were told was true.

Cindy Cohn:
The Carter Page situation is really an anomaly compared to so many others-

Julian Sanchez:
Literally unique. The only case of a FISA Court application being even partly public.

Cindy Cohn:
And that didn't happen because there was a legal system to do it. That happened because of political decisions and so nobody else is going to get that, is the point I think. People should say, "Carter Page found out that there were lies underneath his". I think that it's good to get that input but I think it's unreasonable to expect that that's the only time that's ever happened. It's just the only time we've ever found out about it.

Danny O'Brien:
As a non-lawyer and someone who tries to avoid looking at politics almost all the time these days, could you just explain what Carter Page was and why that was different?

Julian Sanchez:
Carter Page was a foreign policy advisor to the Trump campaign who had all sorts of incredibly sketchy ties to Russia. He was actually someone who was on the FBI, the New York office of the FBI's radar before he had any association with the Trump campaign. They were essentially preparing to open an investigation of him before he was announced as a Trump advisor. When he tried to campaign, this was passed on to FBI headquarters and he, in a sense, they were generally trying to figure out to what extent the Trump campaign was aware of and potentially complicit in the electoral interference operation that Russia was running on Trump's behalf or at least against the interests of Secretary Clinton and because of the panoply of shady connections, Carter Page became the person they thought, this is the one we can most easily target or get a warrant for. We don't want to go after the candidate himself, but and at this point Page had actually left the campaign, but he was the one who seemed to be the most likely, to actually be directly connecting Russian intelligence with the campaign. The most plausible link.

Julian Sanchez:
There was a really disturbing exchange between, I think it was, Marsha Blackburn and Inspector General Horowitz from DOJ, put out this IG report on Crossfire Hurricane that focused pretty centrally on the surveillance of Carter Page and I was very critical of the many errors and omissions and that process, in particular when it came to the renewals of the surveillance of Page. And Blackburn, I think she asked this with the aim that he would say this is incredibly unusual and therefore the only explanation for it is some sort of agenda to get Trump or political bias against Trump. But she asked, how common is it for there to be this many errors and this much sloppiness in the FISA process? Is this out of the ordinary? Horowitz had to, quite candidly, say, "I just don't know. I hope not, but we've just never done this kind of individualized deep dive on a FISA application before.

Julian Sanchez:
We've done audits, but this kind of we're digging into the case file, not just looking at whether the facts in the application matched what was in the case file, but whether there are important facts that were left out and painted a misleading picture. We just haven't done that before so frankly, we don't know how unusual this is". And that ought to be disturbing.

Cindy Cohn:
We do know though, even the programmatic looks at, the Inspector Generals have looked or when the FISA Court themselves has caught the Department of Justice in lies, which they have a lot, that this is really an ongoing problem. It's one of the big frustrations for us in terms of trying to bring some accountability to the mass spying is that the FISA Court ... the part where the FISA Court approves a lot of things that come before it doesn't really bother me as much as the fact that the FISA Court itself continually finds out that the Department of Justice has been lying to them and doing things very differently than they've represented and having a lot of problems and they always just kind of continue to say, "go and sin no more", rather than actually creating an accountability or changes and I think that that message gets received.

Danny O'Brien:
And that's sort of the point where a court like this becomes a rubber stamp because the FBI or whoever is coming to them saying, "we just want to extend this investigation. It's just the same as it normally was." Do you think that the FISA judges get captured in this way, that they just end up spending so much time listening to the intelligence services and the FBI and not hearing the other side of the story, that they just end up being overly reliant on that point of view?

Julian Sanchez:
Absolutely. That's just necessarily the case. I've heard from retired FISA judges that they would hear from government lawyers things like, "you will have blood on your hands if you don't approve this surveillance." And again, because most of the stuff is never going to be public, you have on one side, look, if you are too precious about protecting civil liberties, you have people saying there could be an attack that would kill dozens or hundreds or thousands of people and on the other side, you're never going to be accountable for authorizing too much surveillance because this is not designed to end in a trial. You're never going to be really grilled about why you approved this dubious electronic surveillance.

Julian Sanchez:
I would add that there is a defense intelligence folks and former FISC judges themselves sometimes make of the very high approval rate, which is quite high or you certainly, for most of the court's history, it's been extremely high, 99% plus, though not that much higher, frankly, than ordinary title three applications. And one of the ways that they would defend this and say "we're not a rubber stamp despite this 99% approval rate" is, they would say look, you need to understand how this process really works in practice. Which is, it's not that they just come in blind with an application that we decide. There is this back and forth where they will have a read application, a first draft, and they will go to, not the judges directly, but FISA Court staff, who may be in contact with the judges and say, this is the application we were thinking of submitting and they'll hear back.

Julian Sanchez:
Maybe you should narrow this a little bit, maybe we would approve it for a shorter period of time or for these people, but not those people or we would approve this if you had better support for this claim. And so there is this sort of exchange that then essentially results in applications only being submitted when the FBI and DOJ know it's in a state the FISC is going to approve it.

Maybe they don't submit it at all if the court says, "no, this is not something we would sign off on." And just to finish this point of, which is, and you would think, okay, that would explain it, but the problem is, you've created a process that is guaranteed to result in a FISA docket history that consists only of approvals. So when you get a proposed application and the court says, well, this doesn't quite meet the standard, that application doesn't actually ultimately get submitted.

Julian Sanchez:
It only gets submitted when they know the court is going to say yes, when they've refined it in such a way that the court is willing to sign off on it. The problem is then you've created a body of precedent that consists exclusively of approvals. A particular set of facts where the balance of considerations is such that the court is going to say yes and so then you thus have no record of where the boundaries are of these are the conditions and the fact patterns under which the court will say no so that years down the line, a judge who is looking at applications can say, "okay, here is our record of yeses and nos. Here's our record of what's within bounds and here's our record of what's out of bounds." You only have a history of yes and that is very problematic. You don't have a documentary record of what previous judges have said, no, under these facts that's a bridge too far.

Cindy Cohn:
And so that's why some of the former judges have said, look, this isn't really a court anymore. It's more like some kind of administrative agency. This is what you do if you want the FCC to approve a license. You can have this back and forth and then you finally submit something that works. There's lots of other kinds of bodies that work that way, but courts don't. And courts don't for some good reasons.

Danny O'Brien:
All right, you've said that this court doesn't really have much oversight, but I have heard spoke that there's another institution around the FISC called the FISCR. Is that just like the superlative of the FISC or how do those relate?

Julian Sanchez:
What we really is need is a FISCR. The Foreign Intelligence Surveillance Court of Review is where appeals from the Foreign Intelligence Court go. They've sat, that we know of, maybe a half a dozen times, all in the 21st century. It's possible they sat previously and we don't know about it, but five or six times that the public is aware of and the interesting thing structurally about the FISCR is that effectively the only time they are going to hear a case is on the rare occasions when the government didn't get what they want.

Cindy Cohn:
I have to agree. This isn't really a way that holds the FISC accountable when it makes errors and certainly not when it makes errors that hurt you, the people who are the subjects of surveillance. You know, we managed however, to get some reforms over the years. EFF played a pretty big role in getting some changes to the FISA Court as part of the USA Freedom Act. What's your view on those changes and the impact of them, Julian?

Julian Sanchez:
I think they've been pretty significant. I think we already have cases that we know about where the amicus of the USA Freedom Act created a panel of amici or friends of the court who at least in cases involving novel questions of law or technology can be invited by the court to provide their expertise, provide perhaps a contrary view to the government's argument inevitably why they should have more power to surveil, more broadly. And we already have cases where amici have successfully opposed/proposed surveillance that we know about or identified problems with practices by the FBI. There is, I think, a release made about a year and change ago that was essentially initiated by one of the amici that involved discovery that the FBI agents were searching this bulk foreign surveillance database. It's called the 702 database in a variety of improper ways and essentially taking this supposedly foreign intelligence database and routinely looking for US person information without any real connection to any national security or foreign intelligence case.

Julian Sanchez:
We were probably catching more problems than we were before. It doesn't fundamentally change the structural problems with the court, but it does, I think, make it a little bit better. It has already paid off in ways that are public and perhaps in others that we don't know about.

Cindy Cohn:
I think so too. Honestly, we felt like the first thing we have to do is get more information out about it so that we can make our case that Congress ought to step in and change it because those kinds of changes take a pretty strong lift on our side if we want to try to change things especially because the other side gets to do secret briefings to the intelligence communities.

Cindy Cohn:
The theme of this podcast is how do fix these things. Julian, what would it look like if we got this right. We need to do national security investigations. I don't think anybody would say that we're never going to do those. What would it look like if we got the role of the FISA Court right?

Julian Sanchez:
I mentioned this, I'm not sure this is the right idea, but it's worth putting out the possibility which is just we don't necessarily need a FISA Court. There are other countries that just have all surveillance governed by a uniform set of rules that regular judges are handling. And you could say, applications will go to the whatever jurisdiction is appropriate with the extent that you know one. You'll use the same procedures you use any time a court that is not a special secret court has to handle classified information, which can happen in a variety of circumstances like for example, when you need to prosecute someone for a crime that involves using classified information. But assuming the FISA Court is going to stick around, I think the most important thing that can be done is just remove the presumption of permanent covert.

Julian Sanchez:
The amici, I think, have been very useful, but they are fundamentally a kind of clutch. They are a way of trying to partially reintroduce the kind of back end accountability that is the norm for criminal searches and criminal electronic surveillance in criminal investigations, surveillance

that is criminal. One way you could do that more directly is just by ending the presumption of permanent covertness. I think the idea that electronic surveillance is going ultimately to be disclosed to the target eventually. It's something the Supreme Court has effectively said is an essential constitutional requirement, that one of the things that makes a search reasonable in Fourth Amendment terms is, if not at the time it's conducted then at least after the fact the target of that surveillance or that search needs to become aware of it and have an opportunity to challenge it and have an opportunity to seek remedies if they believe that they've been targeted inappropriately.

Julian Sanchez:
The idea that you can just systematically make a judgment that that's not appropriate, that that's not necessary for this entire category of surveillance targets, even in cases where they do the surveillance and they say "we were wrong, this person was not a foreign agent, we didn't find what we expected", just seems totally misguided. You can't that frivolously dispense with an essential constitutional requirement. There may be cases where you don't want to reveal the surveillance after the fact, especially if we're talking about a foreign person, someone who does not actually have Fourth Amendment rights, but there may be cases where there are some powerful considerations that you should maybe for quite a while not disclose that the surveillance happened, but this shouldn't be the presumption.

Julian Sanchez:
This is something they should have to argue for in the individual case. That, okay, the surveillance is done, why should you not have to tell this US person, and maybe in very many cases, there will be good reasons not to, but it shouldn't be taken for granted. It should be something that eventually they should assume we will in fact have to disclose or certainly if it turns out we were wrong, it's very likely the court is going to make us disclose and therefore, one, introduce the actual check on the back end of people kicking the tires and having the opportunity to challenge surveillance they believe is improper. But also on the front end, creating the understanding on the part of the people who are submitting these applications that you cannot assume this will be secret. You cannot assume that you will be accountable if you've targeted, especially an American, either on weak evidence or a selective arrangement of the evidence. I think that would go a long way toward aligning incentives in a much healthier way.

Cindy Cohn:
I totally agree. I certainly, from your mouth to the Ninth Circuit's ears, because we have that very question up in EFFs case concerning national security letters, which do empower the government to request information from service providers and then carry what is essentially turning out to be an eternal gag on those companies. I completely agree with you that having something, the public having a little sunshine, be the disinfectant for some of the problems that we've seen can be very helpful.

Cindy Cohn:
I also think that I'm not quite sure why we need a secret court hand selected by the Chief Justice of the Supreme Court to do this. Our Article three judges do handle cases involving classified information. We have a very special law called the Classified Information Protection Act that

governs that and people are not regularly leaking classified information out of the federal courts. So I feel like it might have been reasonable in 1978 to think that that could be a problem. I think now in 2020 we have a lot of experience with regular courts handling classified information and we don't see a problem there. We might be able to help a little bit by broadening the scope of the judges involved from the hand picked ones.

Danny O'Brien:
Isn't this also part and parcel of fixing all the problems around the FISA Court, reforming the classification process because I think that something you've identified, Julian, is this dark black ops world of government where the default is to classify information and then just the rest of government which has this presumption that it should be exposed to public review and we've got this creeping movement particularly around surveillance where the presumption is classification. And there's no external way of challenging that. The same people who want to conduct these programs are also the people that determine whether they are secret or not.

Julian Sanchez:
I think that's absolutely right and it's one of the reasons I think the FISA Court has the appearance of a regular court. You always hear when people criticize the FISA Court, they say, "these are regular Article three judges." But in a lot of ways, it is sort of potemkin court because it is a court with a lot of the trappings but divorced from the larger context that gives us some reason to have confidence in the output, I guess, of the legal process which is to say, these Article three judges, but normally Article three judges do not exist in a vacuum, they exist in a context of higher courts who will be reviewing their decisions and hearing arguments from whoever lost the case that you ruled on and may issue a bench slap, may overturn your ruling in a perhaps gentle and perhaps somewhat scathing way.

Julian Sanchez:
You have the knowledge that this is something that advocacy groups are going to look at write about, that the legal community is going to write law review articles about that you may find your peers and colleagues in the legal community not making fun of you, but the gentile law journal version of a kick me sign on your back if you write something that's not very well thought out. So you remove all of that context, you remove the review from above, the review, in a sense by a larger community and you remove a lot of the incentives for decisions to be effectively high quality.

Danny O'Brien:
Can I just quickly ask, what's an Article three judge? What does that mean?

Julian Sanchez:
Article three of the Constitution establishes the judicial branch so these are judges who are part of the judicial branch of the American government as laid out in Article three of the Constitution.

Danny O'Brien:
Right. As opposed to FISA, which is really part of the executive almost?

Cindy Cohn:
Article three judges, as Julian said, are judges who are appointed and approved by Congress in accordance with the way the Constitution creates the judiciary. There's lots of other people who are judges in our world who get called judge, but aren't Article three judges. So the magistrate judges who are judges who handle a lot of stuff for judges. Immigration judges. Lots of people.

Danny O'Brien:
Judge Judy.

Cindy Cohn:
Judge Judy. Well, she's a state court judge. But TV judges. Lots of people get called judges and so when people like Julian and I say Article three judges, we mean judges who were selected by the President and approved by the Congress in accordance with the processes that have developed out of Article three. Article three of the Constitution doesn't actually lay all of that out, but that's the process. It's to distinguish from other kinds of judges and the FISA Court is made up of judges who have been approved under Article three. It's just a subset of those that are handpicked by the Chief Justice of the US Supreme Court to serve on it. And for a long, long time, the Chief Justice would generally only pick judges who lived in the eastern side of the country. There were very, very few judges from the 9th circuit, which is where we are out here in California. And the theory was, what if they have to get on their horse and drive to DC to look at secret things. And we made fun of them and so did a lot of other people point out that there are ways that you don't physically have to be in DC and that you can still review classified information because the FBI does it all the time. We finally have one judge from the Ninth Circuit who is on the FISA Court.

Julian Sanchez:
Although by statute, I think there is a kind of minimum number of FISA Court who have to live within, I forget the distance, but it's 30 miles of DC or something like that. But it is a very unusual structure. That's to say, I think it's pretty basically unique. This is a court with 11 judges, all of whom were chosen by one person, John Roberts. And you can say, "they are all people who have been at least approved by the Senate and confirmed to their regular posts", but the composition of the panel is important. They don't usually sit as a panel. They usually, individually, take turns hearing cases. But there is a lot of social science research showing that essentially your peer group matters. If you have a bench that is composed of lets say, democratic appointees and republican appointees that if the majority of judges are conservative, liberal judges on that panel, on that bench, will tend to vote more like conservatives and vise versa.

Julian Sanchez:
Conservatives, or at least someone who started as a conservative, with a bunch of democratic appointees as their peers will come to vote more and more like a liberal and in deed may vote more liberally than the initially conservative judge with a majority peer group of liberals. So the fact that you have people chosen essentially by one person probably not particularly ideologically diverse or diverse in perspective. I know there's a lot more former prosecutors and former defense attorneys who get picked for the FISC. That's probably true for the judiciary in general, it does mean you have not just all the structural reasons that the court is going to be

disposed to be deferential to the government, but also a selection bias in the composition of the court to the extent that John Roberts is favorably disposed toward granting the government this kind of authority and chooses people whose perspectives he finds congenial]. You're going to have a body that probably does not have a lot of very staunch civil libertarians on it.

Cindy Cohn:
One of the things that we did as part of helping push for this amicus rule is to include in the kind of people who can help the judges, technical people, because one of the things we saw after Mr. Snowden revealed a lot of the spying and the government unilaterally made some of these decisions public is that they were not nearly as well reasoned as we had hoped. And some of that may be because the judges don't have the kind of help that they need to do this because of the secrecy and the limitations on access to classified information.

Cindy Cohn:
We were able to get the amicus to include not just lawyers, but also technical people. But I feel like at that point it's kind of too late. One of the things that I think would make, frankly, and this just isn't FISA Court, but I think all courts do a better job with technical issues is if they had more resources to explain how the tech works for them. I think that especially in the kinds of situations around mass spying, which is where we started and where we spend a lot of EFFs energy anyway. These are complex systems and if you're turning a legal analysis about whether how our people are targeted and how target information is collected, you have to understand how the technology works.

Julian Sanchez:
There's some specific rulings related to the bulk metadata collection, both the telephone records collection under 215 and then that prior Internet metadata ruling where looking back on some of these that eventually have became public, the court is effectively saying well, there's a ruling from the late 70s, supposedly Maryland that says telephone records are not protected by the fourth amendment, you don't have a fourth amendment right against your telephone records being obtained by the government because you've essentially turned over this information voluntarily and this is information the company keeps as a matter of course in its own business records. The FISA Court effectively reads that as, communications metadata is not protected. Again, the opinions that have been released are fairly heavily redacted but it doesn't appear to be anywhere where in okaying this kind of very broad collection that doesn't require particularized warrants based on probable cause, anyone who spoke up and said, well, Internet communication does not work like the old phone system.

Julian Sanchez:
All this traffic that is occurring over the network, when you send an email, Comcast does not keep a business record of what emails you sent. Maybe your employer or your email provider has a record like that, but Comcast, as a backbone provider, doesn't have that as a business record you can routinely obtain. You are collecting information that is, as far as the backbone provider is concerned, just content as much as the content of the email itself or the content of a phone conversation would be content. So there is this way in which this technological difference between how the phone network works and how packet switch networks like the Internet work,

that is pretty clearly directly material to whether this important precedent applies and if this precedent doesn't apply, it makes a huge difference because it means what you're doing is essentially collection of content that is protected by the fourth amendment as opposed to collection of some kind of business record that, under this unfortunate precedent, is not protected by the fourth amendment.

Julian Sanchez:
And it's not that you can't imagine some kind of potential argument they would make about this, but what's disturbing is that it didn't even look like the court had considered this. The court had not even factored in, there's actually this technological difference that calls into question whether this is the appropriate precedent. And it's one thing to say, they made a decision about that, that I don't approve of, but it's another thing to say, they have not even factored this in. They are not even questioning whether this technological difference makes an important legal difference because they don't seem to be even cognizant that these two networks operate in very different ways.

Cindy Cohn:
I'm a huge fan of metaphors, but sometimes you read these decisions and you realize that the court actually didn't go beyond the metaphor level to figure out whether that's actually what's going on and just because there are similarities between phone networks and the way emails work doesn't mean that they are actually the same. I wanted to just summarize some of the ideas we've had because, again, we're trying to fix things here and I think that the fixes that we have talked through are perhaps get rid of the secret court all together and let the regular courts handle these cases is definitely worth thinking about.

Cindy Cohn:
Certainly that all of the court's decisions and the material presented to the court would eventually be made public and that the burden is on the government to say why they shouldn't be made public. There is certainly stuff that can be redacted if you need to protect people's personal privacy but the government needs to demonstrate why these things should be private and I would argue they need to do that periodically, that it's just not one and done and then it stays secret forever.

Cindy Cohn:
I think we've talked a little bit about making sure that the judges are chosen differently. That the choice by the chief justice causes real dangers and hazards in the ability of the court over time to really be ... to hold the government to its word and make the government do its work. I certainly think that the, personally, I don't put words in yours, but that the rule of the amici is small but mighty and needs to get bigger so that the court really does have something, especially in cases ... one of the things that we've lost is the adversarial process at the end that we have in the case of regular warrants. If we're not going to have that adversarial process at the end when we decide whether the evidence is admissible, we need to have more of an adversarial process in the beginning so that there is more of a shake out of what they get to do at the beginning since there isn't going to be one at the end.

Danny O'Brien:
We have this to-do list of what to fix and taking notes. We also wanted to try and imagine what this better world would look like if we did manage to fix the Internet. But I want to narrow this down a bit. Julian, as somebody who's a journalist who writes about a secret court and has to do the research to try and map out what's going on there. If we did fix this process, how would your job change? What could you imagine writing about now and presenting to the public that maybe you can't or struggle to explain in the current situation?

Julian Sanchez:
It's already changed significantly. Again, for decades there were basically no FISA Court opinions that were public. And then there were a very tiny handful and now there are dozens of public FISC opinions since the passage of USA Freedom. It's possible to talk concretely about what the FISA Court says on a range of complicated questions as opposed to just merely speculating about the different ways a court might interpret a statute that is, again, often not super clear because it was written before the technologies that now applies to existed. But certainly to have a more adversarial back end would open up, I think, the possibility of evaluating how often essentially they get it right. We just have no sense currently of how often electronic surveillance approved by the FISC is actually generating intelligence useful enough to justify the intrusion.

Julian Sanchez:
We don't authorize wiretaps to catch jay walkers, as a rule. There is a list of fairly serious crimes that are eligible for wiretaps. But in the FISA case, you have a number of definitions of foreign intelligence. FISA orders have to be geared toward collecting foreign intelligence information and a lot of the definitions of that is rather complex multi-part definition are the kind of things you would think. Threats to the national security of the United States, but one of the rather broader ones is information that is relevant to the conduct of foreign affairs of the United States. And so when you're looking back and saying, did we get anything worthwhile out of this, there's a whole lot of communications between people who are not terrorists or spies or criminals that, if they are business people or government officials, or talking to business people or government officials might well in some sense be relevant to the conduct of foreign affairs of the United States, and because you don't have as you do on the, it's a different title three, the Omnibus Crime Control Act of 1969, ordinary criminal wiretaps are sometimes called title three orders.

Julian Sanchez:
In that case, at least, you can say, you did the wiretap, what percentage of these wiretap orders you got resulted in a prosecution, how many of those resulted in convictions and to the extent that you did a wiretap and then you convicted someone of a fairly serious crime you have at least a sense that it was not completely frivolous, that you didn't just invade people's privacy for no reason. We don't have anything like that on the FISA side really. Surveillance ends and then 99% of the time there is no prosecution. That's not the point of FISA or a foreign intelligence surveillance. But okay, they stopped at some point wiretapping someone. Did they get it right? Did they get it wrong? Was the information in the application a fair representation of the facts available? Were they diligent about trying to present a complete picture to the court or did they

only present what supported their desired results? That's all a perspective that we'd be much more likely to have if effectively people who were surveilled but ultimately weren't doing anything wrong had the ability to drag that into the light.

Cindy Cohn:
Julian's point is really well taken. One of the things we've seen when we've lifted up the cover a little bit on some of these FISA Court investigations is how little they get out of some of them. Certainly, in the context of Section 215, which is the mass telephone records collection that, at the end of the day, there was one prosecution against a Somali guy who was sending money home. That was the only one where the FISA evidence was used. And then the Ninth Circuit just ruled in this case, which is called Maolin, a couple of weeks ago that frankly, the government was overstating how much the FISA Court information was being used and essentially was misleading Congress and the American people about the usefulness of it even in the very one case left standing.

Julian Sanchez:
There is absolutely a pattern we see when, whether it was foreign wiretapping, the one component of Stellar Wind was first disclosed. It turned out this had saved thousands of lives, absolutely essential in preventing terrorist attacks and then years later the inspectors general of the various intelligence agencies put out a report that says, actually we dug into this and we talked to the officials and they really could not come up with a concrete case of an intelligence success that depended on this warrantless surveillance that was part of Stellar Wind. With the metadata program after the Snowden disclosures, we heard "no, no, there are so many cases where terrorist plans have been disrupted as a result of this sort of surveillance." And then again a little bit later, not quite as long after the fact and that case happily, we get two different independent panels, the 'Privacy and Civil Liberties Oversight Board' and a handpicked presidential committee looking at this and concluding fairly quickly, no, that wasn't true. In fact, we just couldn't identify any cases where unique intelligence of operational value was derived from this frankly enormous intrusion on the communications privacy of American citizens that, in the rare cases where there was some useful information that was passed on, it was effectively duplicative of information that the FBI already had under traditional lawful targeted orders for a particular person's records.

Cindy Cohn:
That takes me to the last one on our list of things that would be great if we fixed the FISA Court, which is some real accountability for the people who are affected by what happens in the FISA Court. And I appreciate the inspectors general, they have done some good work uncovering the problems, but that's just not the same as really empowering the people affected to be able to have standing, whether it's in a secret court or a regular court and be able to say this information has come out that I was spied on and I want to have some recompense and there's a whole set of legal doctrines that are currently boulders on our way to getting that kind of relief in our NSA spying cases that I think that some more clarity in the FISA Court and some more reforms of the FISA Court would really help get out of the way.

Danny O'Brien:
So this is: "see you in court,in a court that I can see."

Cindy Cohn:
Exactly.

Julian Sanchez:
Exactly.

Danny O'Brien:
Julian, thank you so much for taking us through all of this. I look forward to your weekly column explaining exactly what happened every day in a new reformed FISA Court and look forward to seeing you on the Internet too.

Julian Sanchez:
I am always there.

Cindy Cohn:
Thank you so much, Julian. We really appreciate you joining us and your willingness to get as wonky as we do is greatly, greatly appreciated over here at EFF, not just on this podcast, but all the time.

Julian Sanchez:
Thank you so much for having me. I look forward to catching up with you guys when we can get on planes again.

Cindy Cohn:
Wow, that was really a fun interview. And boy, we went deep in that one.

Danny O'Brien:
I like it. I like it when you folks get nerdy on the laws.

Cindy Cohn:
The thing about the secret court is, even though you can get pretty wonky about it, everyone is impacted by what this court does. This court approved tapping into the Internet backbone. It approved the mass collection of phone records. And it approved the mass collection of Internet metadata. Two of those three programs have been stopped now, but they weren't stopped by the court, they were stopped Congress or by the government itself deciding that it didn't want to go forward with them.

Danny O'Brien:
After those things were made public, even though this whole system was designed to keep them secret.

Cindy Cohn:
Right. It took them going public before we were even able to get to the place where we saw that the court had approved a bunch of things that I think most Americans didn't want. And clearly Congress stopped two of the three of them and we're working on the third.

Danny O'Brien:
I do feel like I'm honing a talking point here and I feel that it is this contradiction with foreign intelligence surveillance court. It's not really a court because there aren't two parties discussing. It's just one effectively. It's not really about foreign data because it's brief has expanded for these programs that are taking place on US soil and can scoop up US persons' information. And I'm not going to say it's not intelligent, but it doesn't have the technical insider advise and intelligence that allows it to make the really right decisions about changing technology. I think that really just leaves surveillance out of its title. That's the only thing that's true about this name.

Cindy Cohn:
It is the surveillance court. I think that's certainly true, and I agree with you about the intelligence, that basically this court really isn't equipped to be doing the kinds of evaluations that it needs to be able to do in order to protect our rights.

Danny O'Brien:
Not without help. I mean, I think getting an amicus role into this and getting assistance and getting what Julian described as this ecosystem, this infrastructure of justice around it, super structure is the important thing.

Cindy Cohn:
And that's the thing that became so clear in the conversation with Julian, is just how fixable this is. The list is not very long and it's pretty straight forward about what we might need to be able to bring this into something that has accountability and it fixes some of the problems and that's really great since that's the whole thing we're trying to do with this podcast is we're trying to figure out how you fix things. And I think it's pretty clear that if we really do need to fix the Internet, we also need to fix, as a piece of that, we need to fix the FISA Court.

Danny O'Brien:
We'll both, after we finish recording here, go off and do that. And if you'd like to know more about that particular work that we do when we're not in the studio, you can go to EFF.org/podcast where we have links to EFF blog posts and work, but we also have full transcripts, links to the relevant court cases and other background info on this podcast. Bios on our amazing guests and also ways to subscribe to fix the Internet so you won't miss our next exciting episode.

Danny O'Brien:
Thanks for listening in and we'll see you next time.

Danny O'Brien:
Thanks again for joining us. If you'd like to support the Electronic Frontier Foundation, here are three things you can do today. One, you can hit subscribe in your podcast player of choice and if you have time, please leave a review, it helps more people find us. Two, please share on social media and with your friends and family. Three, please visit EFF.org/podcast where you will find more episodes, learn about these issues and donate to become a member and lots more.

Danny O'Brien:
Members are the only reason we can do this work. Plus you can get cool stuff like an EFF hat or an EFF hoodie or even a camera cover for your laptop. Thanks once again for joining us and if you have any feedback on this episode, please email podcast@eff.org. We do read every email. This podcast was produced by the Electronic Frontier Foundation with help from Stuga Studios. Music by Nat Keefe of Beat Mower.