Sean Gallagher:

So, our first panel, as Ken said, is about privacy. The amount of personal data that we give away on a daily basis to service providers and to everybody else is staggering, and part of the reason for that is that big data has become an essential element of our daily lives in many cases, both online and off, and it also has become a problem. Things like Cambridge Analytica, and if you happen to a citizen of China, everything you do down to your gait is measured, and we're entering a world now where even more data is going to be acquired on us by core entities who run the services we use and live within essentially. Web 3.0, the metaverse, things like that offer not just an opportunity for us to have other ways interact with people, but also another way for data to be collected about us down to our very conversations and relationships.

Sean Gallagher:

So, how should society balance the capitalistic need, capitalistic desire to monetize our personal data, our private data with the need for us as individuals and as institutions to protect our privacy, especially in this ever increasingly transparent and monitored world? I have, hopefully, a panel here that can start to address some of that. I'd like to welcome to our panel, Kurt Opsahl. He's the deputy executive director and general counsel, the Electronic Frontier Foundation. He represents clients on civil liberties and free speech and privacy law, and councils on the EFF projects and initiatives. He is the lead attorney on the Coders' Rights Project, and he has been a long time participant in the Crypto Wars. Welcome Kurt.

Kurt Opsahl:

Thank you.

Sean Gallagher:

Especially happy to have Runa Sandvik with us. Runa is a security researcher who works on digital security and privacy for journalists and other high risk people. Her work builds upon experience from her times in New York Times, the Freedom of the Press Foundation, and the Tor Project. Welcome Runa.

Sean Gallagher:

And last but not least, Jay Stanley is a senior policy analyst with the ACLU's Speech, Privacy, and Technology Project, where he researches and speaks about new technology-related privacy and civil liberties issues. He has authored a number of blog posts and influential ACLU reports on a variety of technology topics. Jay, welcome.

Sean Gallagher:

So, privacy, not much to worry about, right? So, I wanted to kick things off by, what do we even mean by privacy anymore? We live in a world where a lot of our personal data is the currency we use to get access to services. We live in a world where our purchasing and other activities are used to make decisions about whether we get access to certain things. We've given up a great deal of this as sort of the social contract of interacting with the world in a digital society. So, how do we define what privacy is in that scope, where we have so much data that we're giving away about ourselves on a daily basis? Kurt, you want to take a first swing at that?

Kurt Opsahl:

Sure. I mean, one conception of privacy is sort of the right to be left alone, to have some autonomy in your dealings and what you are doing, to have a personal space in which you can interact, you can have your thoughts, you can do what you do without someone looking over your shoulder, without someone monitoring, potentially judging, potentially taking actions against your interest based upon that information.

Kurt Opsahl:

Now, you talked about the sort of the transactional nature, and I think that's one thing which is being debated very much around the world, for in a lot of places, privacy is considered to be a human right, that it is not a transactional concept that you pay with things for your privacy, and in the U.S., there is more of a transactional view towards this. But, that risks commodifying an essential part of who you are and what your being is.

Sean Gallagher:

Jay, can you hit a little bit on this? I mean, and also I'd like to talk a little bit about how, what we have in the U.S. defers from say, for example, what's going on in Europe with GDPR.

Jay Stanley:

Yeah. I mean, I think that was all very well said, and I think another way to put it is, privacy is having control over what information you reveal and you don't reveal. You think about somebody living in a town in 1900, there were various businesses, and they dealt with those businesses, and they had maybe relationships with the shop owners, and I gave them money. They gave me goods, and that's how it was, and we've completely lost control of our relationship with the companies that we do business with. A lot of it is because there's sort of a land grab going on. Technology has opened up new spaces that allow for data to be collected.

Jay Stanley:

But, there's a lag between when we lose our privacy and when we realize we're losing our privacy and when something can be done about it. I do think that the arc of history bends towards privacy in the long term. There were centuries where the European leaders were reading the mail of nobles and others in the countries, and over time, over the decades, over the centuries, that was ended because people simply could not tolerate living, losing that privacy. I'm pretty confident that we are going to see a long arc of rebellion against what you're talking about, which I don't think we should accept as the status quo. We aren't living in a gap right now.

Jay Stanley:

I think there are certain aspects of privacy that are culturally relative. Some people go nude on the beach, and other people wear burkas, and that's cultural or whatever. But, there is a core of privacy that people must have. They must have the ability to have intimacy, to be able to have politics and say things to some people that other people don't hear, and a sense of control over their identity and their identity formation, and so forth. So, I think that, in the long-term, I'm optimistic, even though in the short-term, it's terrible.

Jay Stanley:

And the United States is among the most wild, Wild West countries in the world. We're the only big sort of major country that doesn't have an overarching privacy law. I think Congress is sort of pregnant with such a law right now, but we don't know when it'll give birth and what the baby will look like, and I think that's been true since the Facebook scandals, the Cambridge Analytica scandal, but it still hasn't happened. But, that matters. That matters a lot because if you don't have a baseline of expectations that's set by a national standard, then there's not stability of expectations.

Sean Gallagher:

Runa, I wanted to ask you specifically about some of the things you've worked around. I mean, everybody has a different risk model associated with their privacy. I mean, there are certain things we're willing to share, and there's certain things that we don't want to share, but different people have different risks associated with even basic information being revealed. Can you talk a little bit about how you see the risk models associated with privacy? What needs to be protected, and how you've tried to do it with people you've worked with, having worked with the journalists for example?

Runa Sandvik:

Sure. So, just listening to what you were saying, I think what came to mind is that, there is this sort of almost like a constant arms race between what the companies are trying to do or doing because they can versus then what people are saying that they either like or don't like. And so, someone is always going to try to do one more thing, and then see what happens and see who yells the loudest and who yells first, and I think that, in the context of reporters, trying then to figure out who needs what, in what country, for what project, in what context, it becomes really, really challenging to do at scale.

Runa Sandvik:

And so, the type of guidance that I would typically give would be to actually go and look at the privacy and security settings that are available on different sort of social media platforms, just so at least you are aware of what is available and what you can use, and also what's not available to you. So, you can make a decision then of how you want to use the app.

Sean Gallagher:

Yeah. So, it seems, as somebody who works in security right now, and I do threat research on a regular basis and look at what gets exposed in breaches and things like that. One of the things that strikes me is that companies make it so hard to protect your privacy, and applications aren't doing a very good job at protecting your privacy. Can you sort of walk through, what is the baseline right now for being able to do privacy? What level of knowledge do you have to have in order to protect your own privacy?

Runa Sandvik:

I think that comes down to, what is privacy to you, and I think, even just looking at how I've used Facebook, for example, back in the day, like 12 years ago, I said, "I am never going to be on Facebook ever." And then, my friends were like, "Runa, you're moving to London. And so, you have to get on Facebook, otherwise we cannot stay in touch." I'm like, "Fine." I got on Facebook. But, I was very clear. I don't want to be tagged. I don't want any photos. I'm just going to use it so that we can stay in touch.

Runa Sandvik:

And now, like 12 years later, tagging, checking in, asking questions, interacting with the people who are actually still using the platform, and I think that for me has just sort of come with a greater awareness of the settings available to me, what Facebook is doing, what I know, and what I can control. But, that's sort of something that's evolved for me individually over time.

Jay Stanley:

I think that there's a certain amount that an individual can do, but it is a very real arms race, especially in the ad tech area where literally people start deleting cookies, and ad tech brings up new technology, which is very consciously trying to one-up people who are trying to protect their privacy. There's certain things you can do if you're savvy, but at the end of the day, a lot of privacy is just social. It's something that we have to decide as a society that we are going to protect or not to protect, and there's only so much you can do as a human being, as an individual reasonably, partly because of network effects, and partly because of just the sheer time that it would require to click through contracts and so forth.

Kurt Opsahl:

Yeah. I mean, I think it is a challenging thing. Security is one of the areas which has not... It's an unsolved problem, and it has been maybe even a worse unsolved problem over time. But, we need all of these things. We need to have technology that helps secure data encryption to make it, even if data gets out, that it's hard for other people to see it without getting the appropriate permissions.

Kurt Opsahl:

But, I think as well, having a legal and policy regime that supports privacy, to back that up because what we don't want to have is that the only way you can have privacy is go to a cabin in the woods and live off-the-grid. People should be able to interact with society, do the things like be able to talk to their friends over the internet, have these communications, go to stores, and still have some of that privacy and dignity that they have been having for a long time and want to have again. So, we need to have the technical, legal, and policy systems set up to enable that.

Sean Gallagher:

So, there's been a lot of pressure and a lot of change technically recently focused on things like child pornography and on getting into communications to screen for harmful content, and also there's always been this constant push from the law enforcement community for what has been referred to as the Golden Key in crypto and to make crypto backdoorable by law enforcement for law enforcement purposes. Those of us who studied math understand that, that's a problem, that cryptology doesn't work that way.

Sean Gallagher:

But, I wanted to sort of get a feel from you on what the pressures are right now facing communications, and how do we find a balance between private communications and allowing moderation of content, for example, harmful content, especially on apps like WhatsApp or on Facebook Messenger, where Facebook has been a major contributor to information for child pornography. They've been able to break up child exploitation rings based on content that was in Facebook Messenger app, app content. So, what is the balance? How do we find that balance, and how do we avoid bad math?

Jay Stanley:

I mean, I think there's, especially when it comes to computers in the computing world, there's often a search for sort of totalizing solutions. We need to stamp this problem out a hundred percent, but we live in a messy world. We've always lived in a messy world. We have money, but it gets counterfeited. We have crimes here. We have crimes there. I think that there's an impulse sometimes when things move to the digital world to try and use that transition to solve all problems a hundred percent in a totalizing way, and to refuse to accept some messiness as the cost of retaining other values. So, you have to balance law enforcement, and you have to balance privacy, and you have to balance other values, and as we move to digital, we're going to throw the privacy overboard, and we're going to get all of everything else.

Jay Stanley:

Law enforcement, we simply cannot give up encryption because you need to have a right to have private conversations, and you need to have a right to have security. Giving up encryption in the way that's been proposed by law enforcement agencies would be a huge hit to security, as I'm not a security expert, but as all the security experts will tell you. But, it's also a huge hit for privacy. I mean, you can have a private conversation if you walk into the middle of a field with somebody or in the middle of a swimming pool, like in the movie Traffic. But, the question is, should there be a digital equivalent, somewhere where you are not being listened to, and law enforcement would like to get rid of those spaces.

Jay Stanley:

We don't want a world in which you have no guaranteed privacy online, and we think law enforcement will always have many, many tools. They are in no shortage of tools in which to investigate perpetrators of illegal content like child pornography. They have warrants. They can investigate known leads. They can use old-fashioned shoe-leather techniques, and it's a golden age for law enforcement because there's so much data, as we've been talking about, about so much things. And yet, they are seeking purity and perfection and are willing to throw privacy overboard in order to achieve it, and I don't think that's the right balance for our society.

Sean Gallagher:

Runa, you want in on that?

Runa Sandvik:

I completely agree. I think that, when we talk about this debate between online privacy and encryption and harm, there's a lot of stories that are then written about the harm that is caused, and I think that it would be great to sort of flip that around and talk about, what is it that these things are actually enabling for us, and what would it be like to grow up in a world today where you do not have privacy online? What would that actually look like? Yes, maybe you do get rid of crime and some of the messiness that you just talked about. But, in terms of just being a human being and growing up online, very online, what does that actually look like?

Kurt Opsahl:

And I would say, privacy and encryption in particular enables not just privacy, but it enables things like the freedom of association, to be able to have communications with other people. It enables your free expression as you are making statements that perhaps the government might not like, things that might be lawful, or at least in accordance with human rights principles, should be lawful. And then, you have

places around the world, we've been seeing this in Russia recently, where you can't even say the word war. You can't describe their war as a war. And yet, there are people who at least are having some encrypted communications there, and this is a good thing. We have to have a society in which people can have a private conversation, where they can share their thoughts and ideas with the others in a way that we always have been able to do.

Kurt Opsahl:

And as Jay was pointing out, we're in a golden age of surveillance. Law enforcement has more tools available. There's a thing in your pocket that gives your location at all times, and law enforcement can go get that information from a cell tower. This is an incredible difference in privacy than we've had ever before. And yet, law enforcement comes along and says, "We need to have more. We need to have more. We need to have more," to get to that totalizing effect. But, I think if we don't have these private spaces, we'll be fundamentally altering the character of our society, and to give up on the fundamental human rights that encryption enables in order to have total surveillance for total law enforcement isn't a good trade-off.

Kurt Opsahl:

And you talked about a balance, but I don't think that's really the right term for it, and I see that a lot. You'll say, "Well, the balance is to find a way in which we can have encryption, but yet get to the plain text," and as you know, like mathematically, that's not very good. But, the balance discussion of it, framing it as a balance loses sight of the fundamental human rights that are at stake.

Sean Gallagher:

Yeah, good people on both sides. Any promising technologies out there to help fix any of this? Anything new on the horizon or anything that's out there right now that can help us do a better job with privacy? I've seen a lot of people bandy about the idea of using tokens as ways to communicate anonymously, either in a web environment or in the... And then, there was this, whatever they're calling Web 3.0 now. I'm not sure what it is. It's some buzzword, but there is-

Runa Sandvik:

I mean, Elon said that he wanted encrypted DMs on Twitter. So, if that happens, I would say that would be a very good thing.

Sean Gallagher:

Yeah. That would be a good thing. Anything else out there that's nascent that has any promise?

Kurt Opsahl:

Well, there's a trend for some of the messaging services to add or strengthen their encryption. Facebook Messenger is planned to be encrypted and I think Telegram is on the rise. It has not end-to-end encryption. I hope that they do it. DMs getting end-to-end encrypted would also be a good thing. So, there's one aspect of that. The other is that having more controls on your devices to protect it. So, being able to, for example, on your operating systems with your phone, to turn off or limit the advertising ID, the means by which you are being tracked on various things. This is something that has been rolling out more so, but giving people a little bit more control over their lives of whether they want to be tracked.

Kurt Opsahl:

And it's very interesting when Apple made it opt in, instead of opt out for the being tracked, turns out not very many people wanted to opt in, right? The answer is that people actually don't like this. And then, this is not really a new technology, but what I'd point out there is that, advertising based on the content in which the ad is placed, as opposed to tracking the individual that is going there, sort of contextual ads. There have been a number of studies showing that there do a decent job of succeeding at the advertiser's goal with a lot less tracking. There may be other ways in which people can have commerce, advertise their goods, try and convince them to buy it, which don't involve tracking everybody's moves.

Kurt Opsahl:

And this notion of being able to know everything about someone and then provide them with the perfect good, or the perfect pitch for the good that they don't need, isn't necessarily where we need to go. For many decades, we had advertisements on TV that were determined by Nielsen's surveys, a percentage based on what the demographics of the audience are. The advertising industry thrived in those times. Products were sold. It was a successful society. We can go to ways in which are less privacy-invasive and be able to continue on and have a decent commerce.

Sean Gallagher:

Well, and it's also leading to our next conversation after this, which is security. The fact is, is that all that data that's available in advertising networks about location, things like that, is available to a lot of people and not just the advertiser. Anybody can buy it. So, how do we deal with that? I mean, it just goes beyond just individuals shutting off their locations data. There's such a mass of location data available that can be in the wrong hands and for the right price, or it can be stolen. How do we deal with the ethics of handling the data that companies already have?

Kurt Opsahl:

One of the more challenging things is for people, one of the things you want in terms of your private information, to have some idea what's happening with it. But, under many models, that is collected, sold, resold, packaged, and provided, and it is extraordinarily different with someone who doesn't basically study this field to have an idea of where their data is going once it has gone to the first person, and there may be some ways of trying to track that. Data protection regimes in many places in the world try to address that. But, under a system where, once your data is out, anything can be done with it, makes it very, very hard to even understand what threats to your information might be, and you might not have thought by using your phone with an advertising ID, this would mean that anybody with enough money can geolocate where you've been.

Sean Gallagher:

Jay, how do we fix that?

Jay Stanley:

I mean, I think I was going to say what Kurt said, which is, I mean, you have to stop the data from being collected in the first place because once the data is out there, it becomes very, very hard, much harder. There are ways, but it might become much, much harder to deal with, and I think that there's this misconception that the bad privacy world that we have today reflects sort of the sum total of all of our

individual choices, like we're all atomistic individuals, and it sort of produces this as an emergent quality, like mathematically emergent quality. But, we live within structures, structured by corporations and government rules and so forth, and I think that, that is the root of the problem.

Jay Stanley:

People share enormous amounts of information when they surf the internet, but polls also show that they're deeply uncomfortable at the same time with the amount of information that they're shedding, location data and other data. And so, there is this disconnect, but a lot of the discourse around privacy acts as if it's all a product of our individual choices, when those choices are very, very structured, and we're forced into choices, even though we feel uncomfortable about it.

Sean Gallagher:

So, how much of the fix for all this is technical, and how much of it is policy? What do we need to do policywise? What do we need to do technology-wise to make this work easier for people?

Jay Stanley:

I mean, they have to go hand in hand. I mean, I think encryption is a core of protecting privacy, and there have to be policies that don't attack encryption and that allow encryption to be set up in ways that make it work because even though the math can't be broken, you can get around it in different ways. But, I think, in my mind, most of it is policy because most people are never going to be technically savvy enough to, on their own, make use of the technologies that exist to protect their privacy. It has to be part of how we structure society.

Sean Gallagher:

Runa, for the average person, how do you approach this? How do we make it easy for the normal person to do this, to privacy? It's not like click this button, I make my-

Runa Sandvik:

I wish. I mean, it, I think, on some level does come down to the company deciding, just because we can, should we, and actually having that debate up front, trying to then figure out how do they actually want to make money in the long-term, and what are they okay with doing right now? I think for the average person, it's like, yeah, you can dig into some setting on Facebook and figure out what your interests are and how Facebook then serves you ads, which is interesting to take a look at. But, I don't know if most people fully get exactly what that means and what that says about them and also where it's coming from. And so, it's something that I wish was a lot easier because you shouldn't have to be a privacy or security or a policy expert to feel like you have some sense of privacy online.

Sean Gallagher:

Closing... Oh, go ahead.

Kurt Opsahl:

I just want to add one thing as an example. So, many of you may have noticed when you go to websites these days, you often get a pop-up asking if you want to have cookies or turn off a slider. And then, when you go there again, it pops up again, and it's very annoying, and I think this is done on purpose to wear people down. So, finally we're like, "Ah, okay," and you see a lot of these dark patterns.

Kurt Opsahl:

We talk about, is there a technical solution? Well, a long time ago, there was this notion of the Do Not Track signal that your browser would send out. You would say, DNT is one, meaning you don't want to be tracked, and then they could read that. That signal is sent out by a number of browsers. But, rather than just accept that, the companies are putting up these pop-ups to ask you again and again. If you ever say, "It's okay to track me," they're not going to keep asking about that. It's more in the other direction. And so, there are some methods to try and make these things easier, but people aren't using them because they're trying to defeat these methods. So, I think that's why we need the policy thing now to back up what is possible technically.

Sean Gallagher:

So, I'm going to put a little plug in for Privacy Badger since I'm a heavy user of Privacy Badger. It does break some websites I find, but that's because they do heavily depend upon tracking cookies, whether their own or others, and that's a problem. We've got just about a minute to wrap up. I want one sentence from each of you on what your first wish for privacy is in the next year. What can we do in the next year to make privacy easier?

Runa Sandvik:

Encrypted DMs on Twitter? I'm going to lead with that.

Sean Gallagher:

Okay.

Kurt Opsahl:

I guess, good, strong national privacy law. Well, I'll give a pitch. If you search for Fix It Already from the EFF, you'll see a list of various things, including encrypted DMs from Twitter, that we've been asking for, for a couple years now on how to do it, and I would say all of those things, and try and fix the technologies that we can have as much privacy as possible.

Sean Gallagher:

Well, thank you very much. Thank you, Kurt, Runa, and Jay for joining me on this, and hope you all will follow up with our speakers afterwards. This is a topic we could go on for hours about obviously, but we've had 30 minutes. So, we'll leave it at that, and we'll get ready to bring on our next panel. Thanks to you once again for joining this afternoon.