Episode 001 - #CyberChats Podcast
00;00;05;03 - 00;00;25;18
Jen Langdon:
Hello and welcome to CyberChats, a podcast made by the National Cryptologic Foundation. I'm your host, Jen Langdon, and together we'll be demystifying the world of cybersecurity by talking with amazing cyber fanatics like you, as well as industry professionals.

00;00;27;23 - 00;00;59;00
Our conversations in this episode illuminate the connectivity of our devices and how it's easy for people to find and access information about you. There's just no hiding in a digital world. You'll hear from intelligence expert Eliot, who goes in-depth about how open source technologies - one of them being social media - are used to gather information.

But first, we talk with college student Charissa, who shares a real-life story about how she witnessed firsthand the consequences that sharing on social media had on one of her peers.

00;00;59;28 - 00;01;31;00
But our episode doesn't end with this chat. We have a way where you can test your ability to gather intelligence the same way Eliot does. This week's episode challenge will help you see for yourself just how easily you can find someone starting with a simple picture. Participate on our website https://cryptologicfoundation.org/podcast.

This challenge won't be around for long, so be sure to try it out and then tune in next week for the solution.

00;01;32;04 - 00;01;54;14
Charissa Kim:
Hi, everyone. My name is Charissa. I am currently a junior at UC Berkeley studying legal studies and computer science. And I'd say that cybersecurity - I did a lot of cybersecurity related things in high school, which made me sort of realize, Oh, I want to do something in college, but I also do have a passion for law and going into law school.

00;01;54;14 - 00;02;22;24
So I decided to pick up legal studies as my double major.

Jen:
So you're doing all this coaching and you're basically helping create a nonprofit while attending college, and you're pursuing courses about computers and law. So what is it about cybersecurity that's just driving you to be this passionate? Is there one thing in particular you can pinpoint?

00;02;23;09 - 00;02;48;12
Charissa:
I think what I realized is that every single time I would learn something new about cybersecurity, I would just get so excited because it just reinforces the idea about how important and how fun it is to work with different people and how powerful it is to just learn about technology, especially since technology is advancing so quickly.

00;02;48;24 - 00;03;16;29

And so I'm always just so shocked how there's always so many new things going on with our world, especially just since we're evolving so quickly. And so I think taking these different computer science classes, these legal courses, I sort of know what exactly I want to do in life. And it's not a cybersecurity specialist. It's not like an actual cybersecurity role.

00;03;17;10 - 00;03;41;17
But I do want to pursue being a lawyer in the cybersecurity world. And so I sort of want to do both. And so I definitely know that I want to practice law regarding or specializing in cyber security laws and public policy. So I think it was only because of cybersecurity I was able to know my passion and what exactly I want to do in life.

00;03;42;23 - 00;04;04;15
And also just another thing is that I think cybersecurity - just the idea of it and just learning always reminds me how, regardless of what background you have in technology - even if you have none - it's definitely fine. Because whatever effort that you put in, you can honestly do anything. Like, I just think about my freshman year, and

00;04;04;20 - 00;04;41;09
I'm just like, Wow, I genuinely did not know anything.

Jen:
Yeah, you came so far. I feel like hearing you tell your story, it really empowered you to find, like, who you were and - like you said - what your direction and passion was in life.

So a lot of this information that we've talked about - like your nonprofit work, obviously CyberPatriot, K12CyberTalk - all of this is information I was able to find out from you, not just because I know you, but it's on your social media free, open to find.

00;04;42;04 - 00;05;13;09
So it's kind of what we call, like, you know, open source information. Have you always been mindful of the information that you put out there? I mean, you mentioned that you had only learned about cybersecurity as a freshman. Like, were those things at the front of your mind when you were beginning to learn about them?

Charissa:
Right. And so I think it's actually really cool because I took a human rights class using OSINT - open source information investigation methods.

00;05;13;21 - 00;05;38;26
So we have to use utilize open source information to solve human rights cases at Berkeley. And it's so cool that you're talking about open source information because it was very recent when I took that class. And obviously I think it's very important to be mindful about the information being shared on social media because, like, you can honestly find anything, right?

00;05;39;02 - 00;06;04;18
It's also important to know that, I guess, just being aware about the future impact - because whatever anyone posts on social media can have a long lasting impact on the future, right? I think things like

K12CyberTalk and CyberU Tech, I want to spread it out to social media as much as I can just so people can sort of know more about K12CyberTalk and CyberU Tech and they can actually use these resources.

00;06;04;18 - 00;06;28;27
But I definitely think, like, my own personal information…like, I definitely don't want to be posting my Social Security Number or my credit card information, right? And so another thing I kept in mind is that I enjoy creating content in general. Right? And so I don't know if this is a really well known fact, but I really enjoy creating food content.

00;06;28;27 - 00;06;48;03
So I would go to different restaurants and like sort of like record things and make a food review. And so typically that's like one of my favorite things to do just as a side hobby.

Jen:
Charissa, we are going to need to connect over food. I'm going to need to see these links.

Charissa:
So yes, definitely – like, after this entire podcast.

00;06;48;15 - 00;07;18;22
But I think, like, while I was posting these food reviews, I just kept into consideration that it's important to sort of be mindful about how a post can affect the future.

I have a friend who in high school I believe he made a mistake in terms of, like, what he posted on social media. And a lot of his fans or his followers, like, all dug that up because - social media, there's a digital footprint everywhere, right?

00;07;19;03 - 00;07;43;07
And they reported it to the dean of admissions saying, can you reject his application because of his mistake in high school? And he had to go through a long hearing at Berkeley. And he made a mistake and he acknowledged and apologized for it. But I just felt really bad because whatever you post on social media will always have a lasting impact.

00;07;43;07 - 00;08;09;17
And I think just hearing that story from him just reminded me like, wow, I hope everyone will be mindful about what they post in the future because it could affect college athletes, job opportunities, personal relationships, and so forth. But thankfully, he's still a junior at Berkeley as well, too. So everything got sorted out. But just in general, there's so many stories about, like, what you post and it'll have its history.

00;08;10;15 - 00;08;38;07
Jen:
Everything has a consequence, positive or negative, right? So Safer Internet Day was February 7th, and I was wondering if you had any tips given our conversation about, you know, things you shouldn't share and the long-lasting nature of social media. What would you share for somebody in grade school or in college? Some tips they should consider before posting or making sure you use the privacy settings.

00;08;38;07 - 00;09;13;02

Charissa:
I believe many social media platforms have different privacy settings that allow you to control who can see your posts. And so using those settings can sort of allow you to limit the access of what you post and your personal information. Also, I guess this is very obvious, but just making sure you avoid sharing any personal information like your home address or phone number or any financial information on social media that'll just prevent them from identity theft and online scams.

00;09;13;15 - 00;09;45;13
Some friends I have that make their accounts public on Instagram have gotten catfished – like, different accounts have catfished them. So just be aware of that. I guess another thing is like language. Social media isn't like a private conversation and so whatever you post is permanent. So I guess being mindful of the type of language you use, making sure it's not offensive or considered harmful.

I think just another thing about our, like, 2023,

00;09;45;13 - 00;10;14;07
our generation - cancel culture is definitely real. And so just like being cautious about what you post, I would say, and making sure that you know the people who can view your account, your social media and so forth.

Jen:
Those are great tips.

Charissa, we had so much fun talking with you today and we're going to need to connect over food when we end our conversation.

00;10;14;10 - 00;10;40;14
So thanks again so much for taking the time to chat. We love to keep in touch, so don't be a stranger next year when you graduate and let us know what happens.

Charissa:
Thank you so much. This flew by so quickly.

Jen:
I got to talk in person with self-attributed social media spy Eliot Jardines, who is currently serving as the director of operations and treasurer of the OSINT Foundation.

00;10;41;02 - 00;11;09;28
Eliott's entry into OSINT was from his 11 years in the Army, which led to him being appointed as a senior open source intelligence official. He's also worked for a number of companies and is president of Gnosis Solutions, Inc.

One big takeaway I had from this episode is just how much control companies have over our information. And I hope students like Charissa can use her background in cyber and law to help protect some of our information from being so easily accessible.

00;11;11;19 - 00;11;13;25
So first, what is OSINT?

00;11;14;16 - 00;11;28;00
Eliot Jardines:
So open source intelligence is publicly available information, right? So anybody - any member of the general public could get it through request, observation, or purchase.

00;11;28;00 - 00;11;36;10
Jen:
But isn't technology always changing and advancing? So how do you keep up with that and at the same time become an expert at it? Do you know what I mean?

00;11;36;19 - 00;12;07;23
Eliot:
That's always a challenge because the rate, you know – other intelligence professionals, the technology may not change as often. But in open source, we have new tools that come online, new information sources every single day. To be good at open source, you have to like that evolving, you know, constant change. And then you have to think outside of the box a lot because we don't - we're not collecting this information directly.

00;12;08;01 - 00;12;19;13
We're using something that somebody else put up there. So you have to think very creatively about, you know, who might have a need for this information and where might they have put it.

00;12;20;03 - 00;12;28;12
Jen:
So do you have to be a part of the military to be in this sort of, you know, information intelligence part or to get good at OSINT?

00;12;29;00 - 00;13;00;06
Eliot:
So, no, actually, it's done in a whole bunch of disciplines or career fields. So obviously the military is one. Law enforcement is another. And then on the commercial side, there's a whole industry that does things. Like, we do open source intelligence to protect a CEO, right, or a celebrity.

In the business arena, it's done a lot for competitive intelligence, right?

00;13;00;06 - 00;13;11;13
So if we're both selling donuts and I think your prices are somehow way lower than mine and I'm trying to figure out how that is…

00;13;11;24 - 00;13;14;02
Jen:
Do you hack my Internet, do you go that far?

00;13;14;15 - 00;13;35;08
Eliot:

So, OSINT is publicly available information - request, observation, or purchase. But that publicly available part of the definition is critical because anything you put online is fair game, right? So if it involves hacking, pretending I'm somebody else--

00;13;35;28 - 00;13;40;15
Jen:
And basically accessing something I probably should not have access to.

00;13;40;16 - 00;13;44;24
Eliot:
Right, then that's not open source. But I could go back over there if I wanted to.

00;13;49;20 - 00;14;15;04
Or I could observe. So I could send one of my guys to sit out back for days to figure out who sells you flour and who sells you sugar and whatever. And so that's another area where open sources are used a lot. And then also in emergency management, because people tweet, hey, my house is flooding.

00;14;15;04 - 00;14;39;18
Hey, I really need help. And then we have commercial imagery, which is commercial satellites. You take photos, right? So if you've used Google Earth, that's a great example. And then, you know, the other thing that's not a job but a hobby. There are folks who are hobbyist OSINTers. And so there's an organization called Bellingcat.

00;14;40;05 - 00;15;13;23
So, it's B-E-L-L-I-N-G-C-A-T. Bellingcat. They were hobbyists who started doing open source research to figure out events that are happening overseas. And so they discovered a whole bunch of lies that are perpetrated by, you know, certain regimes, certain governments. So, you know, there's some great examples. When the Russians first invaded the Ukraine many years ago--

00;15;14;22 - 00;15;16;17
Jen:
You're talking Crimea.

00;15;16;19 - 00;15;46;19
Eliot:
Yes, Crimea. Yeah, they shot down an airliner. And so they denied that it was them. And the Bellingcat folks, actually, by looking at web cams and traffic cams and whatnot, were able to figure out what vehicle shot the missile and then backtrack that and they were able to locate, okay, this is the exact vehicle. It's a Russian vehicle.

00;15;46;29 - 00;16;11;12
Right. So how did it get here from Russia? And they went backwards day by day. And it helped that that vehicle had some unique markings on it. But it was a Russian vehicle that was handed over to the separatists there in Crimea. And, you know, they shot it down thinking it was a trainee, an Air Force jet.

00;16;12;15 - 00;16;16;16
And so and they denied it and denied it, but it was irrefutable evidence.

00;16;17;14 - 00;16;36;22
And then, you know, in Syria, the regime used chemical weapons against its citizens. And so I believe they were able to do some research along that. So a lot of these kind of world events where you have regimes who are lying about killing people or arresting--

00;16;36;22 - 00;16;42;20
Jen:
Disinformation and misinformation.

Eliot:
So this is a great tool to use to dispel a lot of that.

00;16;43;24 - 00;17;08;14
Jen:
So our episode today is focused on discussing social media and its involvement in OSINT. And we've kind of touched on it a little bit, but it's also about, you know, ubiquitous connectivity, which is basically how all of our devices are constantly connected and they're connected in various ways and they're connected in a way that allows social media to access our data.

00;17;09;06 - 00;17;19;12
What kind of data are we sharing? Maybe it's inadvertent, you know, maybe I don't mean to share it. So can you give some insight on that?

00;17;19;19 - 00;17;31;19
Eliot:
Yeah. So when we get a TikTok account, a—

Jen:
Instagram is popular.

Eliot:
Yeah. You sign- you agree with--

00;17;31;27 - 00;17;34;01
Jen:
A privacy policy, essentially.

00;17;34;10 - 00;17;39;12
Eliot:
Right. And one of the major revenue streams for these companies is selling information about you.

00;17;40;00 - 00;18;03;09
And so everything that you're doing is building a profile. And so there are a few things. We ought to be careful with what's in the background. The career field in the government is OSO: an open source officer. So our bread and butter is what else is in the picture. Because that might tell me where you're located, right.

00;18;03;16 - 00;18;05;25

Jen:
Like, the pictures you share on your social, yeah.

00;18;05;25 - 00;18;16;12
Eliot:
And so if you're in your room and you think you're anonymous posting something, but in the background are all your certificates or your trophies for this, that or the other thing, we can--

00;18;16;12 - 00;18;22;12
Jen:
This Is my school that gave me this award, or I got this from a club that's local.

00;18;22;12 - 00;18;47;14
Eliot:
Right. And so then we can zoom in, right? And we can use software to help. You know, if it's too fuzzy to read, we can improve that a bit. So that's one thing, right? And then when you take a picture with a smartphone, it now adds geo tags - the coordinates of that precise location. And so you have to be careful in your settings that you don't have that location turned on.

00;18;47;23 - 00;19;18;21
So a good example is there's a Russian tourist. And, you know, he was posing on the beach. Well, behind him were Russian anti-aircrafts battery - you know, the whole system. And so he had that location geotagged. And whether this is true or not, I don't know. I haven't seen the information and I haven't talked to the Ukrainians.

00;19;18;21 - 00;19;30;09
But it has been widely reported in the media that the tourist took that picture and then that that site was bombed by the Ukrainians to take out that piece of equipment. So you have to be very careful - if you're doing any kind of interactions on social media, Instagram and whatnot - that you ensure that that geo location is turned off.

00;19;45;19 - 00;20;14;22
Jen:
But even then - and I'll continue using this example with Russian soldiers using their phones because it is widely known that that has been a problem for them. So, can you explain a little bit how that's happening? Because even if you're a soldier and you take a picture and it's devastated behind you or, you know, there's a just plain building, how can they still find your information, you know, other than like the exact coordinates?

00;20;14;22 - 00;20;18;07
What if they take those off? Can you-- is there still another way?

00;20;18;08 - 00;20;44;10
Eliot:
Yes. So, you know, if you're taking pictures and you turn that off and there are landmarks that are visible, right, then you can- you know, Google, for example, has - I forgot what it's called - but you can go in and compare. You can upload a photo--

Jen:
Google Images.

Eliot:
Thank you. You know, we have automated tools.

00;20;44;10 - 00;20;49;12
And so I don't use that too often. And so it will show you like images--

00;20;49;27 - 00;20;51;19
Jen:
Similar photos.

00;20;51;19 - 00;21;23;09
Eliot:
So then, oh, right. That mountainside or that particular building or that monument has, you know, something unique. And so, you know, the other thing is you start doing detailed analysis. There's a group of hobbyists who are trying to track somebody, and this person took a picture of where he was. And he was wanted. And they figured out it was Canada just based on what was around.

00;21;23;16 - 00;21;51;20
Well, they had an idea he was in Canada and then, okay, well, we know he's in Canada. Where in Canada? Well, they looked and there was a streetlight, and that streetlight was only used in one place in Canada. And they researched it and figured out that it was - let's say it's Montreal. And Montreal has these streetlights that aren't

00;21;53;00 - 00;21;58;24
common anywhere else in Canada. They have their own streetlights. And so they figured that out.

00;21;59;20 - 00;22;02;21
Jen:
So that's one way to kind of narrow it down a lot.

00;22;03;03 - 00;22;33;14
Eliot:
Yeah. And then they had a bunch of volunteers and so they literally, you know, with that photograph, they went to Google Earth, the Street View, and started virtually walking down every single street and boom, because they had a whole bunch of people doing it.

And then, you know, the other way that people get found is something called ad tech, which is advertising technology – that's what it's short for.

00;22;34;09 - 00;22;49;25
Speaker 2
And what happens is we all have cell phones and that cell phone has a unique subscriber ID. So it's not your phone number but your SIM card, the little card that allows you to make phone calls, has a unique number.

00;22;50;00 - 00;22;52;28
Jen:
The card that you get when you go and you register for your phone plan.

00;22;52;28 - 00;23;15;19
Eliot:
Yeah, yeah. That little card that you stick – the little chip that you stick in there. And so that early on was used for advertising, right? So I use Waze to get from point A to point B. That's how I got here. And if I stopped at a stoplight, it will show me ads for restaurants or whatever that are right there.

00;23;15;19 - 00;23;39;12
Right. And there might be a discount. "Hey, we're running a—" you know. And how does it know that? Because it's tracking that location. And they sell that location data to vendors.

When you download an app, any kind of app, you want to go in and turn off in your settings the permissions for that app to have access.

00;23;40;02 - 00;23;41;25
Jen:
And you have to do that with every single one.

00;23;41;25 - 00;23;46;13
Eliot:
Every single one. Yeah. So depending on whether you have an Apple or--

00;23;47;01 - 00;23;47;22
Jen:
Android.

00;23;47;22 - 00;24;19;16
Eliot:
Yeah, the settings are different. So in my phone it says I can block it. I can allow them to use the locational data only when I use it or turn it on. And so nothing I have is set to just unlimited tracking. But all that data is collected. So it won't say, "This is Eliott Jardines' phone number."

00;24;20;11 - 00;24;26;20
It doesn't sell the phone number and it doesn't sell my name.

00;24;26;20 - 00;24;30;17
Jen:
So it doesn't personally identify you. In a way.

00;24;30;19 - 00;24;54;01
Eliot:
Well, that data that's sold, no. But then I can put that together. That's called aggregation, right? I can aggregate that data. And so if I have access to adtech data, I can layer it with a map and I go to Google and I say, I wonder where he lives. I type in the person's name and then, you know, you see addresses.

00;24;54;01 - 00;25;16;10
So then you have my home address and then you go into the map and you draw a box. That's called geofencing. So we're drawing a box around that house, and then it's going to tell you all the subscriber ID numbers, right? And so, well, if I've got kids, you're going to see these subscriber ID numbers go to a school.

00;25;16;11 - 00;25;18;10
Jen:
Because they're all associated with your address.

00;25;18;10 - 00;25;34;21
Eliot:
Right. And so, okay, so if I've got two kids and a wife and two of them go to schools and then one goes someplace else and then one goes to my office, it's pretty easy to figure out which one--

00;25;34;24 - 00;25;37;14
Jen:
Who is who and who's doing what.

00;25;37;14 - 00;25;42;00
Eliot:
And so that data is available for as long as I've had that phone.

00;25;43;00 - 00;25;44;24
Jen:
For as long as you've had the phone?

00;25;44;25 - 00;25;45;24
Eliot:
Yes. So.

00;25;45;24 - 00;25;49;00
Jen:
So who has that data? Is it on-- it's not on your phone.

00;25;49;00 - 00;25;50;14
Eliot:
No, right.

00;25;50;14 - 00;25;53;06
Jen:
It's the applications that are storing that information.

00;25;53;06 - 00;26;13;06
Eliot:
Yes. And the phone companies. So, you have a phone. And many times a second, it's pinging the local cell towers. Right. And it says, hey, here I am. Do you have any messages for me? Do you have any

phone calls for me? That's how it knows. That's how your phone rings, right? And so that constant, many times a second,

00;26;13;10 - 00;26;14;10
Hey, I'm here--

00;26;14;18 - 00;26;15;16
Jen:
Constant communication.

00;26;15;16 - 00;26;40;25
Eliot:
Right? It's a footprint of everywhere you've been, everywhere you've gone. And so the software, if it's sophisticated enough, will let you see previous days. And so I don't remember what the exact date is, how far we can go back, but it's a number of years. So the data is there. And it's advertising data, but it's being used by lots and lots of people.

00;26;41;08 - 00;27;04;25
Jen:
Is it really that dangerous that it's being shared? Let's put it that way. Because from a company's perspective, like, yeah, they're able to sell you things, but it could, as they say, well, we want the customers to have a great experience. And you mentioned how you used Waze to get here and it gave you ads from at a stoplight, like, where you could go.

00;27;05;02 - 00;27;06;12
I mean, isn't that beneficial?

00;27;06;22 - 00;27;33;00
Eliot:
Yeah. And so, you know, this kind of geolocational data, being able to fix someone's location on the earth, can be super helpful. Right? But we've got to be careful in how we use that and understand who uses this information and what are they using it for. You know, it's commercially available data so people can buy it.

00;27;33;11 - 00;27;39;06
And some companies are very rigorous in who they'll sell that data to. And others don't care.

00;27;39;10 - 00;27;44;02
Jen:
So some of this data is open source to a degree.

00;27;44;25 - 00;28;06;09
Eliot:
Because you can purchase it, right. So if the public can purchase the data, then it's open source. So it can be used pretty effectively. Where you run into trouble is when that company sells the data to a broker and then that broker

00;28;06;21 - 00;28;17;23

Speaker 2
And then they'll sell it to anybody. Right. And so now you gave Instagram the permission to use your your data because--

00;28;17;23 - 00;28;20;00
Jen:
Right. We signed the privacy policy.

00;28;20;00 - 00;28;23;27
Eliot:
Right. But you don't know that they turn around and sell it 25 other companies.

00;28;23;27 - 00;28;48;19
Jen:
Exactly.

One of my favorite OSINT tools is Google. Google just knows so much and it sometimes knows what you don't know and it knows way more than you want to know. We talked earlier about Google Images, so I was playing with that before we talked today and it's a tool that can also let you find websites for any picture that you enter, right.

00;28;48;19 - 00;28;58;04
Like the original website, among other things. From a privacy standpoint, how do we look at these sort of open source tools?

00;28;58;19 - 00;29;30;09
Eliot:
Yeah. And so, you know, a long held or long-established legal principle is if you're out in public, you have no expectation of privacy, right? So if you're out on the street, then that's open and fair game. You can take pictures, you can take video. You know, a lot of times there are people who will video and somebody will walk by and say, you're not allowed to use my footage.

00;29;30;09 - 00;29;40;12
Delete that. And that's not how this works. If I'm on private property, that's a different story. But if I'm on the sidewalk filming runners going by--

00;29;40;12 - 00;29;42;16
Jen:
In the street or whatever, right.

00;29;42;27 - 00;30;08;01
Eliot:
And so, you know, careful what you post and then who you tag in those posts. And this goes not only for kids, but for parents. We're all very proud of everything our kids do, but-- because once it's out on the Internet, it could be there forever. Right? Chances are. And so, you know, as young people, we all did stupid things.

00;30;08;18 - 00;30;17;27

But I grew up in the previous millennia and that stuff wasn't around. So there are no videos of my stupidity.

00;30;17;27 - 00;30;21;00
Jen:
Not documented on the web, right, because there was no web.

00;30;21;01 - 00;30;43;23
Eliot:
Yes, because there wasn't. But that's a whole different reality today. And so my concern is more in putting all this information together. And so the less information you put out there, the better you are. A few years ago, Facebook was a big-- they'd have these cute little, Oh, what kind of personality are you?

00;30;43;23 - 00;30;45;09
And then what kind of this or that.

00;30;45;09 - 00;30;46;28
Jen:
I think some people still do that stuff.

00;30;47;00 - 00;30;51;05
Eliot:
Yeah and so they'll ask some pretty interesting questions in there.

00;30;52;07 - 00;30;54;02
Jen:
What was your first animal as a kid?

00;30;54;11 - 00;31;01;14
Eliot:
Right. So a lot of those are actually password recovery prompt kind of questions.

00;31;01;15 - 00;31;02;15
Jen:
Oh, for sure.

00;31;02;15 - 00;31;21;20
Eliot:
So a lot of times you're giving away data that-- you know, it's kind of like when you drive by and you'll see a minivan, right? And it's got Bob, Suzy, Johnny, you know, and then the kids. So you see the parents and they have their names.

00;31;21;21 - 00;31;22;15
Jen:
Their little pictures on the back.

00;31;22;15 - 00;31;30;21

Eliot:
Right? And then the little pictures and the names of each kid. And then the name of the cat or the dog or whatever. Like, why would you do that?

00;31;30;21 - 00;31;32;02
Jen:
Yeah, that's so detailed.

00;31;32;13 - 00;31;39;06
Eliot:
That's data nobody needs to know. No stranger should be able to look at a car and call your kid by their name.

00;31;39;26 - 00;31;56;00
Jen:
Elliot, thanks for sharing all this awesome information with us today. Is there any last things you want to share, I guess, to prevent your information from being shared out there? Any last words or tips that you would give to our listeners?

00;31;56;25 - 00;32;29;15
Eliot:
Yeah. So again, check your settings, right? So they don't need your geolocational data to function, many times. Be careful what you post. Think about what you post before you put it on there.

And then just in general, keep in mind that anything that you post could be available for the rest of your life. If we posted a bunch of stuff that you did when you were seven to the Internet, you probably at 14 wouldn't think that that's—

Jen:
Amusing at all.

00;32;31;03 - 00;32;41;29
Eliot:
And then, you know, parents, as well. So I'd encourage kids to have a conversation, right? "Mom, I don't want you to put my stuff up there." And that's a valid reason.

00;32;42;04 - 00;33;04;06
Jen:
It's a valid request.

Thanks again so much. Those are awesome tips that you shared and great information in general.

Stay tuned, everyone, for a video of Eliot and I- we are going to show you how to hack this week's episode challenge. So come back and join us.

Jen:
That's our show! Thanks so much for being a part of our community.

00;33;04;06 - 00;33;30;14
We can't wait to see how you do with this week's episode challenge. Go to the CyberChats podcast page on our website at www.cryptologicfoundation.org to find this week's challenge, submit a question, and join our focus group to help improve the podcast.

You can watch more of this podcast on YouTube. Be sure to like and subscribe to hear more and check out the show notes for more details and links.

00;33;30;14 - 00;33;47;15
This podcast is made possible by the Chilton Foundation.