SECURITY NOW!

Transcript of Episode #525

Disconnect

Description: Steve and Leo cover a relatively small bit of news of the week, including dispelling an unwarranted concern about LastPass being hacked. Then they converse with Patrick Jackson, co-founder and chief technology officer (CTO) of Disconnect, about his company's view of the web-tracking industry, its past and probable future.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-525.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-525-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Lots of security news. He's found some kind of cool information about iMessages, Apple's messaging platform, and how secure it may or may not be; a canary you can use to detect unauthorized access to your stuff; and we'll interview the CTO of Disconnect.me, a new tracking blocker that's available on desktop and mobile. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 525, recorded Tuesday, September 15th, 2015: Disconnect.me.

It's time for Security Now!, the show where we protect, or attempt to, anyway, you and your loved ones and your privacy online, not always easy. Steve Gibson is here at GRC.com. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always.

Leo: And today an interesting show.

Steve: Well, yeah.

Leo: Not that they're not always interesting, but this is - I'm looking forward to this.

Steve: We don't, we almost never have guests on the show. But in this case there's a company and product which has interested me for some time and sort of been on my radar, and that's a company known as Disconnect. And what's interesting is that when I first learned about them, I saw that they were founded by a group of guys, some of whom used to be at Google, and even before that at DoubleClick, the famous huge online web advertising network. And so anyway, as we're sort of exploring and wrapping up all of this discussion about tracking and third parties and blocking content and so forth, I didn't want to leave this until we'd had a chance to talk to somebody from Disconnect. And so we've got Patrick Jackson today, who is one of the cofounders and the chief technology officer, the CTO of Disconnect, whom we will be interviewing in the second half of the show. So...

Leo: Nice. Do you use Disconnect? Do you recommend it over uBlock Origin or...

Steve: Well, I've had them both running - I'm sort of looking here right now at it. And it does pick up things. As I mentioned last week, you can have multiple filters in your system. And uBlock Origin is able to pull the Disconnect list. So in the same way that it's able to pull the Adblock Plus list, I believe it's able to also pull the same list that Disconnect uses. So you sort of have a superset there. But Disconnect breaks it down in a little more user-friendly fashion. And their whole deal was not just to disconnect tracking from browsing, but to provide visibility into it.

So, for example, their main deal is to show a simple little counter, just to let people know how many other domains than the one they're at their browser has just pulled from. So the idea is to educate people and then also to provide some tools for giving some control of this. So they're sort of complementary. But mostly I sort of, you know, we sort of talk about tracking from a theoretical standpoint. I wanted to get somebody who's in the industry, who's actually involved in this, which is why I wanted to actually have a breathing body on the show for a change.

Leo: Involved in the sense that they're blocking tracking, not that they're doing it.

Steve: Yes.

Leo: Yes.

Steve: Right.

Leo: I suppose someday we should get an advertiser on. You've talked about that, too, yeah.

Steve: That would be - yeah.

Leo: See why they do all these nasty things to us.

Steve: That would be good. So we're Episode 525 about Disconnect. Top of the show I have a big mea culpa regarding the fact that glass is not a fluid. The question about whether LastPass has been hacked. Matthew Green's update on iMessage, which was a note that I had known about and you also found, Leo. Then you also found an interesting link to canary tokens that I want to talk about.

Leo: Oh, good, Yeah, I thought that was kind of cool.

Steve: Really cool. And then Let's Encrypt has an update on their schedule, we've got some miscellaneous tidbits, and then our discussion with Patrick. So I think a great podcast once again. So apparently I'm the last person to find out...

Leo: Glass is not a liquid.

Steve: Glass is not a fluid. Oh, my goodness. In fact, as the tweets began coming in - and I have, I've collected, thanks to our listeners tweeting me, every URL the Internet has that discusses this long-resolved myth or urban legend, as some call it, that glass is a fluid, as I misstated last week. So for the few listeners we have who didn't immediately say, "Wait, no, it's not," I wanted to correct the record.

Leo: And I didn't correct you, even though the chatroom was going crazy, I mean, they gave us links and everything, because I lived in an old house for most of my life. We lived in two or 300-year-old houses, and the glass was very much thicker at the bottom than it was at the top. So...

Steve: And now I know why that is, too.

Leo: I thought it was flowing.

Steve: It's one of those - yes.

Leo: Really slowly.

Steve: That's what we would think. It turns out that the old process of glass pane production was called the "crown glass" process, where a lump of molten glass is rolled and blown and expanded and then flattened. And then finally it's spun into a disk. Well, the nature of the centrifugal force spinning this glass in order to spread it out and thin it out means that it ends up being thicker toward the outer edges. So when it is then cut into sheets, it is not uniformly thick. And the people who then mount the glass in its frame deliberately put the thick part at the bottom because it's structurally stronger, presumably, at the bottom. And so that's why the glass is thicker at the bottom - not because it flowed ever so slowly over time, but because it was always thicker from the start.

Now, I really had like a head-slapping moment when I realized, oh, my god, of course it isn't flowing because you could never spin it as a platter in a hard drive. I got myself into this whole pickle talking about how the newer platters that used to be aluminum are now being made of glass because it's possible to make them so much smoother.

Well, it turns out, I mean, centrifugal force is nothing to sneeze at. In fact, it is very difficult to produce a flywheel that can spin at very high speed without pulling itself apart, so much so that some of the flywheels which have been designed for storing potential energy for one brand of electric cars that we've talked about years hence, I mean years ago, they actually used individual strands instead of a big solid disk because it turns out a solid disk sort of like self-crumbles at high speed. So there's no way that, if glass were a fluid, you could spin it from the center and have a stable medium on which to, I mean, where it has to be really stable, on which to store magnetic material. It would, like, increase in size over time until it's sort of rubbing on the edges of the hard drive.

So I happily stand corrected. I apologize for not having any idea what I was talking about. I mean, this is what I learned. I was absolutely sure of it, and absolutely wrong. So thank you, everybody, for making sure that I know. I know many, many, many times over. And it's a good thing that normally I know what I'm talking about. Otherwise my mistakes would create trending topics on Twitter just pretty much immediately.

Okay. So a lot of concern about the news of the next Black Hat, which is in the Netherlands, of course, in Europe, around the middle of November, the 12th and 13th of November. Everybody's concerned because, in the early prerelease of the program, there is a talk planned on the topic, "Even the LastPass Will Be Stolen: Deal With It." This is a presentation by Alberto Garcia and Martin Vigo. So has LastPass been hacked? No. Is there anything broken with LastPass? No. What these guys did was or should be obvious to us, but it's a great topic for the podcast. And it's sort of about the issue of security boundaries.

If you run LastPass in the "remember password" mode, that is, where you have enabled "remember password" as a convenience for yourself so that you're not having to type the LastPass password in every time you want LastPass to be able to access your database of passwords in order to fill in a form, if you have that turned on, then what that means is LastPass has the information available to it without anything from you in order to do that job. Okay. So that means, if something malicious got into your browser and had access to the LastPass code in your browser, and was able to watch it work and watch it perform these decryption processes, then it could have access to your database. And so it's like, yeah. Well, we all know that. Or we should.

So this is, again, one of these classic instances of the tradeoff between security and convenience. All anyone has to do to protect themselves against this particular reverse-engineering-based, it's-always-been-there problem, is turn off, or don't enable, the "remember password" feature. In that case, malware can't statically glom onto anything in your browser and get a hold of your LastPass database because there's a critical piece of missing information which you provide on an as-needed basis.

SQRL, for example, has that fundamentally built in. There isn't a "remember password." We've had some people complaining in the newsgroup about why do I always have to give it something every single time? It's like, because of this. And I've made it very simple to do that, absolutely minimal, but I refuse to drop the barrier completely because it would open it to exactly this kind of attack. And so there is a tradeoff in convenience and security.

And so if users are concerned about this - and again, remember, this is not a remote attack. This is not somebody somewhere else who's able to reach across the Internet into your browser. This requires that your system already be compromised with a problem. And frankly, nothing is designed to withstand that. If you've got something in your machine, then, for example, it's able to get your browser transactions before they're encrypted on the way out and so forth, and have access to the static storage in your browser.

So this is an interesting piece of reverse-engineering. It's a great teachable moment. But this isn't the discovery of a massive vulnerability that nobody knew about in LastPass. The design is solid. But the tradeoff for the convenience of just going to a page and having the form, your username and password, magically filled in for you, is that your browser, without any input from you, can do that. And so that inherently means that, if something were to get a snapshot of it from the inside and then reverse-engineer the plugin, they could do that, too.

So I wanted to make sure everyone knows this because there have been, as this Black Hat program has spread around, and about halfway down the page is this scary-looking, yes, your LastPass can be hacked. It's like, okay, but there's nothing to see here. And if this...

Leo: Now, I ask LastPass to - so on my desktop I have to reenter the password. But I have it set up so I reenter it only every 24 hours. That's just as bad.

Steve: Yeah, unfortunately, I mean, what we really want to do is keep things out, to keep bad things out.

Leo: You want to enter a password every time you want LastPass to fill in a form, basically. What if it asked for a PIN? What if it says, well, not the full password, just a six-digit PIN? Would that be adequate? Because LastPass offers that as a feature.

Steve: Unfortunately, it sounds like that would be open to brute force. And for that matter, so would your password. So you do need your LastPass password to be strong.

Leo: How about a fingerprint? So on iPhone, or phones that support fingerprint readers, I have LastPass set to remember my password, but to require a fingerprint authentication before it fills. That seems like that would be adequate.

Steve: That is super solid, yes.

Leo: Okay. Because I don't want to have to type - see, this is the problem. I have a long random password.

Steve: Right.

Leo: I don't want to have to type that every freaking time.

Steve: Right.

Leo: Fingerprint's good.

Steve: Fingerprint's good. And what I did for SQRL is to make an interesting compromise because we have this thing that makes brute-forcing incredibly difficult. It's called EnScrypt, which is an algorithm that I designed. Essentially it uses the scrypt password-based key derivation function many times so that it doesn't take milliseconds, but it actually takes seconds. But you only have to do that once. So like the first time you're turning on your computer or you log in, you have to give SQRL your entire long password. And then you sit there for five seconds while it verifies it. And this is a memory-hard function that there is no way to short-circuit. But you only have to do it once. From then on, it only requires that you give it a hint.

And so essentially what happens is, after performing all that work, it takes a snapshot and reencrypts it using just the front of your password, like the first four characters. And it does still use a one-second-long "enscryption" so, again, even that cannot be brute-forced. But a single mistake in guessing wipes the information it's using out of memory and requires you to then enter your whole password. So it's a careful compromise to keep the system easy to use.

So when you're logging into a website, you just go bing bing bing bing, four characters, and it says okay, fine. But somebody walking up to your computer, if you just run off to make coffee, they can't log in as you because they won't know what those four characters are. And any mistake, and it puts you back and requires your full password. So all of these things inherently have a tradeoff. But, Leo, this is only true until we get, for example, biometrics on Windows machines. We have them now, for example, with the iPhone and Android.

Leo: Whew.

Steve: Yeah. So Matthew Green has spoken up. He, of course, is the well-known cryptographer we're speaking of often. He was the person who managed and helped sort of put a public face on the TrueCrypt audit, both phases of that. We speak of him often because he's very much active in crypto. In the wake of the news that we talked about last week, where the State Department, or the Department of Justice, I'm sorry, the Department of Justice was pursuing Microsoft for getting access to mail that they were storing over in Ireland, and also the DOJ was upset with Apple for denying a subpoena for access to iMessage, Matthew decided he wanted to revisit iMessage's security. And for those who've been listening to me carefully, there's nothing new here. But it was good to hear it from Matthew. And so I wanted to share, without changing a word, just the beginning of what he says in his own words because this is, again, sort of one of our main fundamentals of ease of use versus security tradeoff.

So Matthew says: "How does iMessage work? Fundamentally, the mantra of iMessage is 'Keep it simple, stupid.' It's not really designed to be an encryption system, as much as it is a text message system that happens to include encryption. As such, it's designed to take away most of the painful bits you expect from modern encryption software, and in the process it makes the crypto essentially invisible to the user. Unfortunately," writes Matthew, "this simplicity comes at some cost to security.

"Let's start with the good," he writes. "Apple's marketing material makes it clear that iMessage encryption is end-to-end and that decryption keys never leave the device. This claim is bolstered by their public security documentation, as well as outside efforts to reverse-engineer the system. In iMessage, messages are encrypted with a combination of 1280-bit RSA public key encryption and 128-bit AES, and signed with elliptic curve DSA, digital signature algorithm (ECDSA), under a 256-bit NIST curve." He says, "It's honestly kind of ridiculous, but whatever. Let's call it good enough."

And by that he means, when you send "Hi Mom," you know, that's what happens to it. This is like, oh, my god, you know, there's no way anyone is going to decrypt your "Hi Mom" message. And he says: "iMessage encryption in a nutshell boils down to this: I get your public key. You get my public key. I can send you messages encrypted to you, and you can be sure that they're authentic and really came from me. Everyone's happy." And then he finishes, or the last part of what he wrote I will read, and that is: "But there's a wrinkle. Where do those public keys come from?"

And so my way of phrasing this is, in any modern cryptographic system we know that the keys provide the security, that that was the innovation in cryptography where, rather than making the algorithm secret and trying to have a super-secret encryption algorithm that no one could ever figure out, we realized that just doesn't work. Everyone is going to figure it out.

So instead, we have public encryption algorithms that everybody knows and that smart cryptographers can check and verify and pound on and work to break. And instead those are keyed so that, first of all, one algorithm can be used with a virtual infinitude of keys in order to create an infinitude of virtual algorithms, essentially. So we know that the keys provide the security. So the bottom line on the security of the system as a whole is, if you delegate responsibility for the keys, you delegate responsibility for the security. If the security comes from the keys, and you delegate that responsibility, then you have delegated responsibility for the security.

So as we've discussed, and as Matthew just reminded us, we're trusting Apple and their key server to only provide us keys to the people we're intending to send our message to. If they provided us with the FBI's public key, in addition to the public keys, for example, of all the other devices that we have that are synchronized through the cloud and through iMessage, and the public keys of the people we're talking to, all of those public keys allow those recipients to decode the message that we have uniquely encrypted to their public key. But we don't know that there isn't an extra key among those unless we look.

And so Matthew brings up the point that Apple does need to behave themselves because the protocol, messy as it is, has been reverse-engineered. There are tools available that at least show the public keys that we have and that messages are being encrypted under. And if someone really went to the trouble, they could do this at all endpoints and figure out which keys were which and who belonged to whom. So again, the good news is, as he says, it's meant to be an easy-to-use, not-in-your-face messaging system. And as we will hear Patrick mentioning later on because we have a time machine that lets us know what the future holds - and I just lost my train of thought. Patrick will be saying something about this.

Leo: In moments.

Steve: In moments.

Leo: All right. We should explain. Now you've let the cat out of the bag. We earlier today recorded an interview with the CTO and founder of Disconnect.me. And he'll be on later in the show. And he'll say something that Steve is about to refer to, but doesn't really remember.

Steve: Exactly.

Leo: Because it's from the future. You can't go back to the future.

Steve: It's not really that clear. It's coming to me, you know, but not with full clarity. So I'm dimly aware of something that Patrick will be mentioning in the future.

Leo: He will be mentioning it. Just listen carefully, and you'll recognize it.

Steve: And so, okay, so this is why I remain bullish about Threema, because everyone wants to know, is iMessage secure enough? Is Telegram secure enough? And it's like, yes. I mean, it certainly is.

Leo: Secure enough.

Steve: That, yes. Is it as secure as it could possibly be? No, because the only way for any system to be as secure as it could possibly, well, okay. If we really want to go to extremes, and Leo, this is your favorite position, well, you'd have to write it yourself, compile it yourself, you know, know cryptography.

Leo: You might want to check the BIOS code.

Steve: Oh, yeah, you know. And then you'd have to, like, transfer it by camel to the recipient, who installs it and then uses it so that you absolutely are responsible for every phase of that. Okay. If we simply trust the Threema guys, then what Threema does is transfer all responsibility for managing the keys to us. Now, I just - I send texts to my mother and my sister and my friends. So I'm not that concerned about the security of iMessage. It is secure enough. But if I were - I'm not sure that I would text state secrets, period, just because...

Leo: That might not be a good idea.

Steve: Too many other things that could go wrong. I mean, for example, notice that, when I'm texting, I'm happening to use the swipe or swish or whatever it is keyboard, whereas Apple replaces it with their own whenever they see that I'm entering a password. Meaning that I'm entering stuff into iMessage through a third-party keyboard which Apple feels is not safe enough to enter something as secure as a password. So the reality is there are all these stages where something can be compromised. You don't, you just cannot utterly trust an electronic communication system today. There are just too many ways that something could interfere.

So I would argue, if you like the idea of managing your own keys, and understand that there's going to be some inconvenience, Threema lets you do that. If iMessage and Telegram and their autonomous key management, I mean, they've got crypto. They're doing the best job they can. It is secure. No casual eavesdropper is going to get your stuff. And the FBI is unable to see what you have communicated because Apple, they got tired of that multiple month waiting list of decryption requests for subpoena-grabbed or whatever-grabbed iPhones. Remember years ago Apple had this backlog of iPhones they were decrypting for law enforcement. Finally they just said, you know, no. We're going to put technology in this so that even we can't do it. And then we just say no. And so that's where we are today. So I thought it was interesting that Matthew reminded us where these tradeoffs are because it's all about tradeoffs.

So, Leo, you found an interesting link that I followed up, and I thought I would share with our listeners, well, because it also plays into one of the other sort of evolving themes of security, which is, if you cannot protect it, at least monitor it. And so this is a site called CanaryTokens.org, which sort of takes an interesting position: C-A-N-A-R-Y-T-O-K-E-N-S dot org. CanaryTokens.org. And what they do is they generate tokens like encrypty-looking URLs, such that, if anything ever attempts to access that URL, you will be notified. And so, for example, you could put this in an email to yourself with a saucy-looking subject and leave it unread in your inbox. And if anyone ever opens that email and clicks the link, you will know it. And so it's sort of a form of honeypot. And in their FAQ they acknowledge that, if somebody were to block CanaryTokens.org, then it wouldn't be able to make the query, and so - and they say, yeah, of course. I mean, and so this is sort of meant to be a free and fun service to allow people to create honeypots of all sorts of different types. They talk about how...

Leo: Although they give you the source code, so you can - they encourage you to run your own server.

Steve: Exactly. And that's the way to do it is not to, exactly, is not to be relying on a well-known domain that could get blacklisted by bad guys, but to create, use a domain you have, or create one, if you want some way - or, I mean, you could just use an IP address, if you have a static IP, also. The idea being that - and what I like about this is that on their web page they say, "Don't learn of your breach from CNN. A fully functioning honeypot in under five minutes." And the idea being that, again, the lesson we're learning, and this is why I was talking about the need for IOT, you know, the Internet of Things things, to be able to somehow keep themselves updated, that it's incumbent upon the manufacturers of firmware of things that are going to be on the Internet to be able to fix them when the mistakes are found because everything we know tells us that mistakes will be made, and they need to be correctable.

Similarly, everything we know tells us that it is, for a sufficiently motivated intruder, it is impossible to keep them out. They can pound on you. They can send your staff phishing emails with custom-designed email, designed to get clicked on. One way or another, they can get in. So if that's the case, then the next best thing you can do is to detect that intrusion as quickly as possible. And so IDSes, Intrusion Detection Systems, they've been around for a long time. I really think they're growing in popularity. Well, in fact, evidence demonstrates it because people are recognizing that, wow, you know, what we need to be able to do is respond quickly in the event of a breach, which we can only do if we're notified of a breach.

So anyway, this CanaryTokens.org is like a cool free service that allows you to play with the concept. I mean, and you can just, you know, you can create the tokens for free. They ask for your email address, not to send you spam, but in order to provide you with notification. And it's just sort of fun. And you could also, for example, use that link in your own little web bug or email bug, hook it up to an image on an email that you send, and you get notified if somebody opens the email. You know that they did.

Leo: It's so cool.

Steve: Yeah, it is.

Leo: What I do is I have a file called passwords.txt that I put in all my Dropbox folders. And that way, if that gets opened, and I figure once it gets in Dropbox, that's the first thing they're going to look for, then I get a little email. Somebody opened your passwords file. What?

Steve: Big, big honeypot.

Leo: What?

Steve: The other thing I learned by researching this was that this practice of bugs goes back to the early 1900s. There were things called "map bugs," where professional cartographers needed to essentially protect their maps from forgers, from people who would come along and not invest in the tremendous resources of cartography, of like where the streams meander and where the roads are and where, I mean, think about back in the early 1900s, how difficult it was to create maps, but how easy it is to copy somebody else's.

So what did they do? They made up cities. Like, somewhere on a road they'd put a town that didn't actually exist. And then, if they found that somebody else's map ever appeared that had this fake town on it, they knew they had proof of where that town came from. It had to have come from them because they made it up. They put a map bug on their map. And in fact some of the early mapmakers were able to go to court and demonstrate that successful forgers had done that, which I thought was really interesting.

Let's Encrypt, the project to automate the complete management, the requesting, the verification, the issuing, the usage, essentially the entire lifecycle of the least assured class of web certificates, the so-called DV, the Domain Validation certs, is on schedule. First certificates - it's not in wide public use, so don't everybody go running out right this second. But first certificates were issued, as they hoped, in early September, last week actually, the week of September 7th. And they are, over the course of the next 10 weeks, between September 17th and mid-November, November 16th, which is when they expect to have full general availability, they're going to be cautiously and slowly ramping this up.

If you really want to be part of like the early experience, you can contact them, get your domain whitelisted for acceptance by the Let's Encrypt server, install the software in your web server, and have it issue the request to the Let's Encrypt server, which then challenges it to verify that your server is in control of the domain by putting something up on a page, which Let's Encrypt then verifies, showing that you have control, or that that server has control. And then, on the fly, it synthesizes a certificate and provides it to your server. And the Let's Encrypt software on the server side installs it and brings up HTTPS, just like that, and then automatically renews it as its expiration date approaches from then on.

So I'm really excited about this. This still leaves the organizational verification, the OV, and the extended verification, the EV certificates, as the proper domain of the certificate authorities, as they should be, because there, there are additional tests and representations being made by the ownership of those certs that you are an organization that they have checked out or that an extensive background check, much more extensive than just you, you know, GoDaddy issued a domain, and you put a server on it. I mean, that's really the thing I like about Let's Encrypt is that it allows everybody to easily bring up SSL connections with all the benefits that those provide.

So they're on track. They did make their early September startup as they planned. And over the next 10 weeks they'll be ramping up to full speed. And soon anybody who is saying, oh, I'm not encrypting because it's too much of a hassle, that's gone; I object on principle to the idea of paying for the privilege, that's gone. And so I really think probably even Richard Stallman would use this system in order to have...

Leo: Well, let's not go crazy.

Steve: ...TLS connections. In a little miscellany I wanted to mention that Jon Schiefer's movie that we talked about quite a while ago, "Algorithm" - this was the hacker movie that our listeners back at the time really liked. It's at, like, 1.65, probably, million viewers. It's free to watch. It's on YouTube. For anyone who doesn't know about it, it's a 90-minute movie that gets all the technology right. Jon is a viewer of the podcast, and he says that the podcast inspired the movie. So I just wanted to bring - I've got a link here in the show notes. The movie is called "Algorithm." And you can go to TheHackerMovie.com, that's sort of his anchor for this, and I think you can watch it there, or it'll take you to YouTube, where it's doing really well, and deserves to. So a fun movie.

And so, Leo, my opportunity to quip briefly on last week's Apple news.

Leo: Oh, good.

Steve: Two things.

Leo: Love to hear your opinion, yeah.

Steve: Yes. Unfortunately, the iPhone is pink.

Leo: Yes, it is pink [groaning].

Steve: I know. When I saw it, it's like, ooh, that's not what I think of when I think of rose gold. That's definitely pink. And the iPad Pro does look big.

Leo: Oh, it's big.

Steve: Yeah. And so I think I'm going to probably punt on both of these. I don't think they're going to get money from me this cycle.

Leo: Well, you don't have to buy a pink phone, you know. They still offer steel and titanium and...

Steve: I know that, of course. And I did go for the gold one, and they offer a gold one. Except my phone is still new.

Leo: Yeah.

Steve: And I don't think I'm going to jump on the brand new phone every year bandwagon, either. Now, that's subject to change. I will eventually go to an Apple store and play with the new phone UI and see if I can't live without it. But for me, the iPad is my goto device. And what I'm hoping for is that, if I wait another year, maybe two, that they will backport the pen technology, the stylus technology to the original smaller size iPad. Because it just - I really, you know, I drop it into a case that fits. I schlep it around with me. I just don't want to be carrying this big monster slate. I mean, it really - for the pro user, it is great. I'm drooling over the stylus. Many people tweeted me after the Apple event, saying, well, Steve, you got the stylus that you wanted. And it's like, yes, I did, but not on a pad that I want to carry around.

So I'm really - and I agree with you. I listened to you on MacBreak Weekly just before this, Leo. I'm excited to see what happens. I love the idea that we're going to probably get a new class of professional software that matches the pro-ness, and the stylus. It was fun to listen to Andy just going gaga over the thing. I just would like all of that in a smaller form factor. So I'm hoping that maybe Apple will say, hey, you know, we can sell more of these if we put this technology in the regular size pad.

Leo: Yes. I don't see any reason why they wouldn't. But we'll have to see.

Steve: Yeah. And I've heard you mention a number of times Soylent. And I just close my eyes. I've been aware of Soylent from the beginning.

Leo: It's Soylent 2.0 now. Don't - this is not your grandfather's Soylent.

Steve: That's correct. And it's not made of people, either.

Leo: No.

Steve: So for those who don't know, Soylent is this wacky concept from a guy who just - I remember watching his first video. And he said, "Eating is boring, and it takes time, and it's annoying, so I want to create goo which replaces all of that."

Leo: Haven't we always wanted People Chow? If they can make a dried kibble that can keep an animal alive with its total nutrient package, why can't they do it for humans?

Steve: Yeah, I think it's that every so often the dog gets table scraps.

Leo: You can do that. You can have a hot dog once in a while.

Steve: Well, and so I just want you to promise me, Leo, that if you start drinking Soylent for lunch, you will still have breakfast and dinner.

Leo: Yes. I would never live on this. And people have tried. Although that was on Soylent 1.0.

Steve: That's this guy's mistake. I salute his inventiveness. But from everything I've learned in my decade of research - and believe me, I would normally be right there, where it's like, oh, cool, you know, we know enough in order to replace food - and the answer is no. We do not know enough. I mean, we know enough to...

Leo: Macronutrients we can supply. It's the micronutrients.

Steve: Like for a week in space or something. But, yeah, exactly. There are so many phytonutrients in plants, there is so much more going on that we have no idea about. And they are crucial. So, yeah, to fill your stomach and keep you from having to put a bunch of vegetables in the blender, then maybe.

Leo: I'd still put the vegetables in the blender, if I were you.

Steve: Glad to hear it. That was a...

Leo: It's actually tasty. Think of it as a protein drink, as a smoothie.

Steve: Yeah.

Leo: Yeah. It's got isomaltulose in it. I mean, what could possibly go wrong?

Steve: Oh, I bet it's got all kinds of stuff.

Leo: Algal oil.

Steve: Do not try to survive on it.

Leo: No, no. I never have planned to do that.

Steve: I salute the guy, and just the concept. But the idea that you could replace food. You know, I mean, and he never poops. And I'm thinking, okay, I don't know that that's completely...

Leo: I don't know if that's the case. You have to. There's got to be some...

Steve: Well, no, but he doesn't.

Leo: This guy doesn't poop?

Steve: At least with version one, there was nothing coming out the other end because...

Leo: That sounds like a terrible idea.

Steve: And believe me, his body was saying, oh, thank god, we will use all of whatever you give us.

Leo: Everything. I'll take it all.

Steve: Because all we've got is this strange goop that you've consumed.

Leo: Well, and the first version was highly glycemic. He's addressed that. I don't, you know, I think this is probably not a good idea. But I enjoyed it. I enjoyed it.

Steve: No, it's really not. It's just it's fun. I just like, you know, you've got to love the world and the Internet for bringing us the news of something so crazy.

Leo: I always thought we should have People Chow. Not maybe every day. Maybe once in a while you go out to a nice meal. But there should be just something you could snack on. I don't know.

Steve: Yeah. Well, you have several...

Leo: They're making me take phosphatidylserine, whatever the hell that is.

Steve: You have several sponsors who provide you with boxes...

Leo: Delicious snacks.

Steve: ...of snacks at the door.

Leo: Out of real food.

Steve: Well, speaking of the Internet, I will just share one short little tweet that I got on 9/9 at 1:13 in the afternoon from Jim Howard, who just said - I appreciated the tweet because it was, like, on the fly. He said: "SpinRite just saved the day again." He says: "I paid my dues today, and it saved data off a volume that a whole team of admins had given up on."

Leo: Wow.

Steve: "Thanks for making me look like a rock star." And Jim, thanks for letting me tell our listeners to remember SpinRite, If they ever run into trouble, or if they want to keep themselves from having trouble in the first place.

Leo: So smart people - that's the challenge, I can tell you, of advertising on this show, in fact really on the network, but this show in particular, is you guys are smart. Can't put one over your eyes.

Steve: Oh, don't ever make the mistake of telling anybody that glass is a fluid on the TWiT network.

Leo: Exactly. We have a new advertiser, it's called Fluid Glass. Nope, we don't. I did, though, and I should have it by next week, I ordered some gallium, pure gallium, because it melts at 89 degrees. It's a metal.

Steve: Nice.

Leo: That melts in your mouth.

Steve: Okay.

Leo: But don't put it in your mouth. I am going to put it in my hand, though. You know what people use it for is to make trick silverware. So they'll make a spoon. And then you stir it in your coffee, and the thing goes [melting sound].

Steve: Cool.

Leo: You know, I hope it's safe, but who - you know, we'll see. It melts in your hand, not in your mouth.

Steve: Yeah, don't put it in your mouth.

Leo: No. I don't think I'll put it in my mouth.

Steve: You know, we grew up playing with...

Leo: Mercury.

Steve: ...mercury, of all things.

Leo: I did.

Steve: And now - oh, I know. You know, and we had, like, chemistry sets you could buy at the toy store. Now, if a thermometer breaks in the elementary school, they evacuate the county.

Leo: I know.

Steve: It's like, oh, my lord.

Leo: I'm sorry, sir, that's just red-dyed water. You're safe. Don't worry. All right. Steve Gibson, Leo Laporte. And would you like to introduce our guest?

Steve: Yeah. So we've been talking about this whole issue of advertising and counting and remunerating websites and tracking for the last few weeks. And we've beaten this thing to death. But on my sort of list of things to do was to talk about Disconnect because I've been aware of them for a couple years now. And what I remember seeing was just sort of - it was so tantalizing that I thought, okay, we have to talk to somebody there because among the cofounders of Disconnect, what I remember hearing, and Patrick confirmed for me when he and I were chatting briefly to set this up yesterday, was somebody who was originally at DoubleClick, one of the earliest and largest online web advertisers, whom Google purchased.

And sometime after that, they set up a project which was called Disconnect, in order to bring to light the level of inter-website tracking that was going on. And so I thought this was interesting that this was, in this case, now ex-Google people who had done this. And our podcast is heavy on technology. So for years we've talked about the network-level mechanisms by which third-party cookies are managed, and how tracking is handled, and more recently how JavaScripts are being loaded into browsers from third parties to do whatever they want to do.

And I thought, you know, the one thing we're missing here, because we're heavy on theory, was something over on the practical side because this whole - one of the issues with tracking is that it's all sort of behind the scenes. No one knows it's really going on. You visit a website, and unless you have something extra added to your browser to show you what a web page is doing, it's completely invisible. So I wanted to invite, I did invite, and we have, Patrick Jackson, who is a cofounder and the CTO, the chief technology officer, of Disconnect. And I wanted to chat with him a little bit, for the sake of our own edification and our listeners', about like what's happening with this whole tracking industry. So welcome, Patrick.

PATRICK JACKSON: Well, thank you, thank you. Great introduction. And I'm happy to be here, happy to discuss what we're doing at Disconnect and pretty much just the general landscape of online tracking and now kind of the new focus of mobile online tracking, which is getting a big flashlight with iOS9, and kind of people's awareness is going up. So, yeah, yeah. We started Disconnect because we wanted to give folks a choice about their online privacy. And it's hard to have a choice if you don't know, if you're not knowledgeable of what exactly is going on.

And so like the first major component that we want to accomplish is education about online privacy. And so we do that by showing you in real time a counter of what is being blocked; or, in cases where we're not blocking content, but all the third-party connections that are being loaded on different websites that you visit. And so a lot of - there are a few other folks that are doing things like this, like another popular one is uBlock Origins, which you guys covered a couple episodes ago. And these are all great tools. These all bring together awareness of what's going on when you visit different web pages. And we think that's incredibly important.

And one big distinction between desktop and now mobile, which is increasingly - and it's going to eat desktop, if it hasn't already, it's definitely going down that path - is there's not as much visibility. And so I think, just like with a browser, you can right-click and view source of the page. You can inspect elements. You can even bring out certain tools like man-in-the-middle, for more technical folks, man-in-the-middle software to actually figure out what's going on with the websites you're visiting. But it's a lot easier.

On mobile, you don't have that luxury. And so for the past year or so, probably actually last two years, we've been really geared on trying to bring more awareness on mobile, and really get those folks who don't even really realize the importance of online privacy, we try to make sure that they actually know what's going on. Because maybe they don't care, and that's fine. But if they do care, then they should be able to do something about it. And so that's pretty much our mission. And we still have a long way to go, but it's definitely more folks are talking about this than ever before.

Steve: You know, on one hand, a simple question to ask you, what your sense of how much people care about this, except that we'd expect sort of some bias. But for me, the really telling factor is the number of instances of use of these tools. I mean, it's in the millions that these things are being installed. Do you have some sense for, like, population size? And I'm sure you must have an idea of, like, how many people are taking advantage of this.

PATRICK: I think on desktop the exact - I'm pretty sure it's in the millions per day that are installing various types of privacy tools. A lot of those may be adblockers. Some of those are privacy tools like Disconnect and other extensions. But it is, you know, every day more people are kind of being alarmed to, oh, this is what's going on, they're installing these tools. And I think that's what's kind of scary for a lot of folks, including folks like Google, who they're trying to get ahead of the market. Like pretty much desktop and the browsers, it was something that they can't control anymore. You know, they created the APIs that allowed people to build tools like Disconnect, and they created a marketplace for them.

And so they almost - they kind of helped enable this. Which it was going to happen anyway. But they provided the APIs early on. And with mobile you kind of see they're trying to structure, they're trying to control the ecosystem a lot more so these tools can't be created. But you know the will of the people will prevail. And I think, just like Apple is now paying attention, I think we'll start seeing more across other platforms. And in most - a lot of people, their only device is a mobile phone.

And so I think we're going to see, when iOS9 content blockers come out, I think we're going to see enormous adoption. And I think it's going to be bigger than any of the keyboards, you know, when Apple created the keyboard APIs, and even some of the today extensions, I think folks are, regular people are going to start to realize, like, oh, okay, I can start to control some of this. But a big distinction we like to make is we do not want to be an adblocker. We do believe ads are a currency of the Internet. But there should be user choice on how they should be tracked, if they want to be tracked. And so it's first about the education, but then also giving people the tools so they can take action, if they want to.

Steve: Well, you anticipated my next question. I just had it ready because I was going to ask you, differentiate for us, I mean, everyone understands what an adblocker is. So how is Disconnect different from an adblocker? How is it not an adblocker?

Leo: So our focus is malicious third-party content. And we use the word "malicious," and also "malvertising," to note anything that the user doesn't intend to be on the page that they're visiting. They're third-party content. You know, if I'm visiting TWiT.tv or CNN.com, I don't expect a lot of these other third-party servers to be interacting with my machine. And so we focus our blocking on things that are third-party, that are not expected, do not deliver value to the consumer. And so but we do not touch first-party content.

So a good example is, with this netcast, you do have sponsors. And these are people that you have a direct relationship with, that they're interested in your users, they feel that their product will be a good fit for your users. You also vet them, and you say, you know what, I think this is a complement to what we're talking about, the focus of the shows. And that is a direct relationship between you, who's ever

> sponsoring, and then also your users. So that is first-party. That's a first-party delivery of some type of sponsorship or an advertisement. The same is with certain websites like New York Times. They may have their own ads, either talking about their own product, or somebody went to The New York Times and said, you know, I want you to push this banner on your page, but it's a direct relationship between that company and New York Times. We wouldn't block that.
>
> What we're blocking are just the third-party requests that deliver no content, that the user doesn't have a direct relationship with, and it's not delivered via first-party means. So that is the big distinction. And I think a lot of times it kind of gets - we kind of get grouped, enclouded with a lot of the folks who just want less clutter. They want no ads. But we understand that not everybody has money to buy a subscription to a publisher's content. And that's what ads have, you know, they've taken the place of that.
>
> And I think this is just moving folks, these publishers to do things more first-party, things that are - they're a lot more valuable to the user because it comes with a cosign of, you know, if Leo talks about a product, or Steve, you talk about a product, I'm probably going to raise a bigger eyebrow to it and probably look into it, versus, you know, I just get some anonymous, not anonymous, but just some random company who thinks they know who I am, and they want to track me across the web and serve me ads that they think I would be interested in.

Steve: I guess the other issue, and as you and I were discussing a little bit yesterday, is one that since there's been no visibility into what sites were doing, there was nothing to put any back pressure on their conduct at all. And so what we have seen as we've installed some tools that allow us to look at the number of domains that a web page causes our browser to then in turn go fetch things from, is that there's been this explosion of that, where we go to one domain's page, and now we're seeing queries from 45 other seemingly unrelated domains.

And in talking about it yesterday, I think you brought up a really good point, which was that to some degree these websites, because there was zero cost to them to add some random tracking widgets or auditing widgets or whatever, I mean, it's like it's zero cost to them. They put a script tag on the page, and every single person who brings that page up, their browser goes and reads the script tag, goes, pulls some JavaScript, in some cases hundreds of K of JavaScript. And since we talked about uBlock Origin, for example, so many people have sent feedback saying, oh, my god, I can't believe how much faster the web browsing is now, only because all of this non-visible, non-content data is no longer being pulled.

PATRICK: Yeah, yeah. And you're exactly right, like there's a lot of the website owners you talk to, they have no idea. You know, whether it's a WordPress blog that they own, and maybe they just click and install certain plugins, and they don't really realize that those plugins add script tags that, you know, every plugin that you may add creates a new relationship between your website visitor and then whoever owns that plugin. And who knows the privacy policies of those companies, of those plugin creators, and if they're getting paid on the back end to sell user data because they're - it's these hidden companies that are on so many of the websites that people visit.

And so, you know, I think tools like ours also help, if you run a website, to know what exactly is going on, on your own home page. And sometimes we talk to companies, and they're amazed at, you know, I didn't know I had 76 third-party requests that were blocked. And they had no idea who these companies were. And a lot of times these companies may also redirect through other third parties. And so it may look, the first request may look benign. But then once you see, oh, wow, it's actually really going off to this other place. And so, you know, the browsers and the extensions, we've been able to create things that allow users and website owners to see what exactly is going on. And so, you know, I just hope that we can do the same thing for mobile because that's exactly what we need, especially since everything is going that direction.

You know, there's really no simple way that a nontechnical person could do to actually verify what connections that these apps are creating. In the same way that a website owner may just add script tags, developers, they just add different libraries that may give them, okay, this library gives me a new share, a sharing tool, a sharing widget. And then this next one gives me something else. Like they think these are just features. But, no, it's another company that's managing now a new relationship with your own users. And that's problematic because there's no way for you to control and vet, you know, if you're just kind of randomly picking. Or even just adding anybody that's not you. It's hard to maintain what those companies are going to do with your users' data.

Steve: It's funny, you were talking about how the third parties sometimes invoke fourth parties or more. And in fact we can see that, if we are using some tool to control outbound queries. Because, for example, if we're blocking them, then the blocker will say, oh, you know, we prevented 25 domains from being accessed. And then you say, oh, okay, well, you know, I want to let up the blocking on this single site. So you disable the blocking. And now the number of domains is not 25, it's 75 because, in blocking 25 domains, you don't know what domains those domains were going to query. And so as soon as you allow - and so I know that this has confused people. It's like, wait a minute. If I have blocking on, it shows 25. If I have blocking off, it shows 75. What's the deal?

And the deal is that, when you make those other queries, then the code in the data that is returned from that query is making additional queries. And in your example, for example, it might be pulling some JavaScript library from yet another domain, only because there's one function in that library that they want. And again, it doesn't cost these people anything to cause our bandwidth to be consumed, our batteries to be consumed, our browsing experiences to be slowed down. And so I think that's how this has gotten lopsided and sort of out of control.

I did see - I thought this was very interesting. Just in the last day or two, the folks at Adblock Plus were talking about sitting down and having some sort of an industry-wide roundtable discussion between the advertisers and representatives of the blocking and user community to sort of sit down and say, look, things are in trouble here. Ads have gotten obnoxious. People are objecting to them. The full-page takeover? The problem is, it is incrementally more effective if you take over the whole page and annoy someone and force them to hit, you know, go find the little X close button. And it's because it's effective that we're seeing this. But users are not without the ability to say, okay, wait a minute. We've got some technology we can bring to bear. And if this keeps up, that's what we're going to have to do. So as I've said on the podcast in the last few weeks, it feels like, you know, we're in a really interesting time of great change.

PATRICK: Yeah, definitely. And, you know, you hit it right on the head. Like these sites, so if I'm getting ads - I think, to step back a little bit, since there's nobody really regulating this, and it's pretty much been a Wild West from these advertisers and whoever these tracking companies, you know, they've been pushing the line so much, and to the point where a lot of, you know, websites are almost unusable unless you kind of go through some interstitial, or you have to find that small X button to click. You know, they keep doing it. And they've done it in the past with pop-ups. And, you know, and browsers came and said, you know what, this is so annoying, we're not going to allow pop-ups. So by default, you know, Chrome and all the other browsers, they block pop-ups.

And so I think it's only a matter of time. They've shown time and time again that they're going to push it until somebody causes them to change. And so our philosophy is, you know, it should be an opt-in type of relationship. And by default, if you want to start managing your privacy, we'll show you what's going on. We'll block those. And then, if you want to access that content, or you want to whitelist this page, we can allow you to do that. And that's like the most effective way because after the fact the damage is done. The cookies have been set, you know. Even if they're not setting cookies, they're fingerprinting your browser. Like they may have already gleaned whatever intelligence they needed with that initial request.

And so I think it's time for the industry, whether it's Adblock Plus getting a bunch of folks together with the ad industry, something's going to change. And it's not like they haven't anticipated this. And I think no one should feel - I think the only thing that people should ever worry about are kind of the publishers and making sure that they know acceptable ways to guard their users' privacy and not make so many shady deals with just any company that can give them revenue for their visitors because their visitors' data is worth so much more. So I think it's an education process of the consumer, also the publishers. And then the ad networks, they have to evolve, as well.

It kind of reminds me of when, with cellular, companies, you know, for the past few decades they've been eating everyone with the cost of SMS, like it's been a nickel, you know, for an SMS message. And everybody has known that this is ridiculous, you know, why are they nickel-and-diming everyone off the cost of SMSes? And then now you have apps like WhatsApp, you know, iMessage, and Google Hangouts. That industry, they rode that as long as they could until somebody took it, you know, and said, hey, this is not the best way to do it, and you've been overcharging folks for so long. It's not that expensive. Yes, you had infrastructure costs. But you didn't need to overcharge for so long.

So I don't feel sorry for the carriers in that sense. And I think that, if they were, you know, everybody has a chance to see the writing on the wall. And if they aren't taking meetings with privacy companies, and they aren't looking to change up how they're doing, then it's really on their own doing, their future. So I think the ones that we will see succeed will start championing user privacy. And this, I'm talking in the terms of ad networks, they'll start championing user privacy, realizing that they can't track first and ask questions later. It should be more of an opt-in relationship.

It should be much more of a, hey, you know, maybe the user volunteers information. If I know this is a currency that I can use, and the publishers at the end of the day can get paid for this, maybe it's okay for me to tell you that I'm in San Francisco, I'm a male, I'm married, I have a dog, and those are things that I may be interested in getting ads in. But all the hidden tracking, it's just, you know, it's gone far too long.

And I think it's really going to come to a head pretty soon, where regular users who are not sophisticated are not going to take it anymore. They're not going to take their bandwidth being ate up by tons of requests, these rich banner ads that are probably, you know, some could be a meg each. They're not going to take that anymore, and they're going to start installing tools like content blockers or taking advantage of extensions that can help the user manage this. And I think we're on - it's going to happen, really, I think, in the next six months or so, the landscape will look a lot different.

Steve: Well, we had the hope with the DNT header, you know, the famous Do Not Track header. And I was very excited about it, and I talked about it a lot on the podcast because it seemed like a simple signal that we could send. And the criticism, of course, was, well, yeah, but following that or obeying it is entirely voluntary, and nothing compels anyone to do so. But I'm still holding out hope that that may be a way, or part of some sort of a solution where advertisers agree that they will honor Do Not Track. They will sacrifice the cross-site tracking because in listening, because as a consequence of iOS9 adding the API to allow for content blocking in Safari, Leo's been talking about this in all of the shows, podcasts for the last month or so. And I've watched his co-hosts expressing their discomfort with tracking.

So it seems to be that on one side there's the issue of bandwidth consumption. But this whole idea of sort of unseen tracking going on is something that just creeps people out. And I think that, if there can be some sort of an agreement made where someone can explicitly say, you know, I want to support ads, I want to support websites that I go to with ads. But what I don't want is the idea that data is being aggregated about me and sold behind my back. So if I explicitly state that in the headers of my browser, I need to know that that's going to be honored.

PATRICK: Yeah, exactly. And you're right, we are working with the EFF, Electronic Frontier Foundation, on this kind of revisiting DNT because, like you said, it has been, you know, all my browsers, I have it set. But you don't really know what it's doing because it's really just a flag, and you don't know if they're honoring it. So, you know, we're working to make sure that Do Not Track becomes a true reality. And so I think that it's one of those things where I think we have to kind of move on two fronts, like the policy side of like working with them, but then also, you know, if their dollars start to diminish because they can no longer track people like they want to, then I think they're a lot faster to come to the table. So it's, you know, people, these same types of folks reengineered how they presented ads and got rid of pop-ups because these browsers said we're not going to allow pop-ups anymore, they're too annoying.

So I think tackling it from both fronts, we can ensure that we get the attention to address these issues from like a policy standpoint, but then also from just the technical standpoint of you need to make this much more of an opt-in relationship. And I think it also encourages publishers to rethink their current setup for how they're monetizing their pages. And I think the co-founder of Twitter, Evan Williams, he recently said in an article that banner ads are dead, and it's all, you know, going - and they've been dead. But going forward, it's all going to be about native ads.

And I think that way everyone kind of wins. Like if I go to a publisher's site, and it's like a vetted ad that we know, that they know is useful to their readers, I think it's going to have a lot better conversion because it's going to be tailored to that audience. And it's not going to rely so much on individual tracking. But just, you know, I know that you're on Daring Fireball, and you're probably interested in Mac products, so here's a really vetted product geared towards that, that everyone sees. So I think we'll start seeing a lot more of that, publishers getting into more of the native ads.

Leo: And of course that's the model we use at TWiT. My fear is that, A, advertisers are not going to accept that model. They're not going to - so it'll work for Daring Fireball because it's a boutique site. But more importantly, I think it's the end of the free and open web and a move towards apps because none of these blockers work on apps. Apple's blocker doesn't work on apps. The whole movement is going to be towards keeping stuff off the free web, and you using a dedicated Wall Street Journal app, New York Times app, in which they can track you because in fact you have to be tracked in order to get the app. And so all your, in my opinion, and I don't want to beat a dead horse because I've said this a hundred times, you're killing the free and open web.

PATRICK: Well, so I think the web is going to adapt. And I think that, you know, we launched in 2013 the first way to block trackers globally on apps. So if you're in The Wall Street Journal, and they do use third-party tracking services to render ads or just to track you, whatever it may be, we can affect those.

Leo: That works on the iPhone?

PATRICK: That works on the iPhone.

Leo: So if I'm in a Wall Street Journal app, and there's an iAd on there, you're blocking the contact between the iAd and the server? No, you're not. Apple won't let you. Apple won't let you do that; will they?

PATRICK: So, yeah, yeah. But, so, yes. And we figured out a way using completely open APIs to achieve that, where it's completely transparent to the user. They install a configuration profile, and we can affect communications globally where we block it on the device.

Leo: I get it. So you're using, you're basically using a phone profile to say you can't contact these sites.

PATRICK: Exactly. Exactly.

Leo: Yeah. I get it. It's like a hosts file.

PATRICK: Exactly, yes. And now we're pushing to more of that network-level protection because the apps, you know, it's...

Leo: By the way, now I really have to trust you, Patrick.

PATRICK: Well, yes and no. So you have to trust that, when we install the configuration profile, that it has what it says it has in it. But we also encourage our users to validate exactly what we're doing.

Leo: It doesn't work as a man in the middle. I don't go through your servers.

PATRICK: No, you don't. No.

Leo: You're just blocking. You're just blocking the ad servers.

PATRICK: Exactly. We do it all locally on the device. And so you don't have to trust us with your data. So we do offer VPN that achieves the same type of tracker protection. And that's only for users that are in questionable WiFi situations where they can turn on a VPN, and we get all the traffic. But with our iOS app, you install the profile, and you do not have to route your traffic through us. It still goes from Point A to Point B without routing. It just blocks on your device.

Steve: Wow.

PATRICK: And that's really where a lot of - so we also built this same capability for Android because, if you look on the Android app store, there's no privacy tools. We figured out a way, using the completely supported APIs, to build a way, to have a privacy-friendly way to block content. And that app, about a year ago, Google pulled it twice because they said it affected third-party apps, which it was intended to do. We want to block tracking in third-party apps. So right now we're going through an EU complaint because of that, because of them pulling our app.

And so luckily, you know, I think if users can have these types of tools, it's just better that they can make the decision on what they want their mobile phones to do. And if you actually look, if you man-in-the-middle some of the traffic of these mobile apps, you would be amazed at what goes on. I gave a talk at Mozilla, there was a Mozilla festival, and we educated users on how to set up a man in the middle, how to install a cert on their phone so they could actually start logging in, seeing the traffic, even encrypted traffic from apps that they use, and actually putting a face to a lot of these hidden requests.

And folks were just amazed. You know, at the time, this was probably 2014, one of the example apps we used was ber. And there were so many requests to non-ber, ber-owned servers, and they were mobileapptracking.com, you know, mobileconversionwhatever.com. There were so many requests being fired off even before you even created an account with ber. And they do that because they want to track campaigns. They want to see where you came from. They want to try to do all of that. But it's just amazing. And if you have an opportunity, if you're technical enough, do a man in the middle of the apps you use and then see how they're regarding your privacy.

Steve: Well, I'm glad that we have some controls, and I'm glad we have you guys in the industry keeping an eye out for us. So thank you very much, Patrick. This has been great.

PATRICK: Yeah, well, thanks for having me. And I really appreciate you guys inviting me, so thank you.

Leo: Our pleasure. Patrick Jackson. You want to know more, go to Disconnect.me. There's a free version, and there's a paid version, and you can install it on your desktop or on your mobile. Disconnect.me. So you don't need iOS9 to use this now, Patrick.

PATRICK: No. No. We work right now on iOS9, and we're exploring the iOS9 new APIs, but...

Leo: You don't need them.

PATRICK: Our technique, you don't need it.

Leo: Neat. Thanks, Patrick.

PATRICK: Yup.

Steve: Thanks, Patrick.

Leo: Appreciate your time.

PATRICK: Take care.

Leo: Take care. Patrick Jackson, Disconnect.me. Thank you for bringing him on, Steve. I thought that was interesting.

Steve: Yeah, well, I just, you know, we don't often have guests. But these guys had been on, as I said before, on my radar for a while. And I thought it would be fun to hear from somebody who has sort of the tool provider vantage point. And we learned a lot that we hadn't known or heard before. So thank you again, Patrick, for coming on. It was great.

Leo: And you said you use this and uBlock Origin, so you use them both together.

Steve: Yeah, I have, I've been running them side by side for the last couple days, just sort of to get a feel for what it is. My sense is that uBlock Origin is probably right for the techier of our audience, and Disconnect is beautiful for the less techie, just sort of I don't know what to do with all those buttons or a list of all the domain names. So uBlock Origin, as I explained it, is really more of an HTML firewall, and Disconnect is a gentler sort of introduction to what's going on behind the scenes.

Leo: Okay. I'm going to keep using uBlock Origin. I feel like I have to fight to defend websites who rely on advertising to stay afloat, and I do worry about the future of them. But I have to say, yeah, I'm coming more around to your point of view, which is that nobody has a right to force you to see billboards as you drive down the highway. Nobody has a right to use your bandwidth like that and to track you like that without your permission.

Steve: Right. And I think what'll probably happen is that we will, like, as we stagger towards a solution, is that at some point sites will start saying, "You have an adblocker. We require the revenue from ads. So please disable your adblocker if you want to proceed." Then we decide whether we want to do that for this particular site, or click the next link in the Google results and go to a site that doesn't make us lower our shields. So it's going to be interesting.

Leo: I also feel like advertisers got themselves into this pickle.

Steve: Yes.

Leo: By being so horrible.

Steve: Yes.

Leo: And, you know, our advertisers, I think, understand that. So last week, after the show, I flew to New York for something called the IAB (Interactive Ad Bureau) Upfronts, which was the first time podcasts have ever had an upfront. And the idea is you go and present to advertisers your programming and ask them to buy a year's worth of ads, which of course is not how it works in podcasting. It's only how it works in network television, but...

Steve: Wow.

Leo: Anyway, it was really interesting. And one of the things I said, and I looked at Lisa afterwards, I said, "I hope I didn't make a mistake," is we turn down advertisers all the time. I said, "My point of view is that we have a community. And when you become an advertiser, you become an advertiser so that I will make an introduction between you and our community. And you come in as a peer, and you come in with all the cards on the table, and you say this is our service, these are our features and benefits. And if you'd be interested, here's the website." And to me that's kind of the respectful way to advertise.

Steve: And you and I are trading our reputations. I mean, there is some reputation cost to us...

Leo: Absolutely.

Steve: ...for representing these advertisers as being worthy of sponsoring the podcast.

Leo: Well, if somebody buys a product - this happens - buys a product because I said it was a great product, and it doesn't work, they actually don't blame the company. They blame me. Seriously. Who do you blame? You don't say, "Oh, well, those guys are jerks, but Leo's still okay." No, you go, "Leo, you told me this was good, and it's not." So I'm not going to put my reputation on the line unless it's something I really feel is good.

Steve: And I know in my interaction with your staff that, when there's ever an advertiser that wants to...

Leo: Oh, yeah, we take care of them, yeah.

Steve: Well, that wants to consider advertising on Security Now!, I receive an email from Glenn, who says, hey, these guys want to advertise. Are they okay? And so, you know, anything advertising here I had a chance to look at first.

Leo: Everything from Harry's, which you loved. In fact, you couldn't stop doing ads for them, even though they weren't paying.

Steve: And I never really understood why that was wrong. But anyway. I'm like, oh, they're good.

Leo: If we give it away, just remember this, no one will pay for it. Steve is an innocent abroad, and that's the truth. And it's always a pleasure. Thank you so much. If you want to get copies of this show, you have a couple of places to go. Of course Steve's site, GRC.com, is a great place to go. While you're there, pick up SpinRite, the world's best hard drive maintenance and recovery utility. Take a look at all his freebies. Check out how SQRL's coming along. He also has transcripts of the show, so you can read as you listen. Or in fact, I suppose you could just read. I don't know if there's anybody who does that, but you certainly could. And that would make it very easy. There's a nice adblock in transcriptions. You just turn the page. Does she transcribe the ads? No, probably not.

Steve: No.

Leo: No. Why bother?

Steve: Right.

Leo: So if you want an ad-free version, you can read along. Thank you, Elaine, for doing that. Thank you for paying for it, Steve. We also have full quality audio and video of the show, if you should choose to see our shining faces at TWiT.tv/sn. And you can subscribe wherever podcasts are aggregated. And if you want to watch live, we had somebody in studio visiting. He had to take off, but it's always nice to have people in the studio. Email tickets@twit.tv. Or just tune in at TWiT.tv/live about 1:30 p.m. Pacific, 4:30 Eastern time, 20:30 UTC, every Tuesday. Next week questions, you think?

Steve: I think a Q&A. The industry has been quiet, at least until mid-November, when we deal with the fallout from Black Hat in the Netherlands.

Leo: Yeah. So GRC.com/feedback, or Steve's Twitter handle, which is @SGgrc. He takes questions from there, too. But they have to be 140 characters or less. Thank you, Steve.

Steve: Thank you. Actually, they don't anymore because DMs. DMs can be any length, and I accept DMs from anybody. So type away.

Leo: All right.

Steve: Thank you, my friend. See you next week.

Leo: Bye-bye.