EFF: How Facebook Monetizes

Description: After catching up with the past week's updates and security news, Iyaz and I share information presented by the Electronic Frontier Foundation (EFF) which describes how Facebook manages the privacy interactions with their third-party data warehouses and advertisers.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-404.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-404-lq.mp3

SHOW TEASE: Coming up to Security Now!. Leo's out, but Steve is here to give us the updates on Java, the new Firefox, and to find out how you're making Facebook a lot of money, and more.

IYAZ AKHTAR: This is Security Now! with Steve Gibson, Episode 404, recorded May 15th, 2013: How Facebook Monetizes.

It's time for Security Now!, the show that helps you stay safe online. And Leo's obviously not in. I'm Iyaz Akhtar, and thankfully I'm joined by the star of Security Now!, the mustachioed master of security, Steve Gibson.

Steve Gibson: Hey, Iyaz. Great to be with you today on Episode 404.

IYAZ: 404.

Steve: The "missing" Security Now!. The "not found" page of Security Now!.

IYAZ: But this episode is findable, anyway. It's not going to be 404'd. We've got a full episode coming up. I'm a little fried. I'm going to get that right out, tell people right in the beginning, because this is hour, what, five of broadcasting for me. So thankfully Steve's here, and he's the real expert about everything. We've got so many things to talk about, a lot of news coming up.

Steve: Okay, that's true. So what would the second Tuesday of the month be without Microsoft patches? In fact, it would be probably an impossible second Tuesday of the month without Microsoft patches. Ever since they started doing this, they've never missed a second Tuesday of the month. And so certainly that's no difference now.

Now, we talked last week about a brand new, just discovered, zero-day vulnerability that affected only Version 8 of Internet Explorer. Not 6 and 7, not 9 and 10, only 8. So

Microsoft released, I think it was later that day, later Wednesday, they released a hotfix that sort of mitigated the concern. But the good news is they were able to get a patch, a full patch out for that by today.

So they fixed 33 vulnerabilities yesterday on Patch Tuesday for May, including this zero-day flaw. They did it actually in two pieces. They probably already had a cumulative update for IE in the pipeline tested and ready. So the zero-day flaw patch exists in a second update, and probably it makes sense that it's just for IE8, so you only need that one if you're using Internet Explorer 8 on your system. Otherwise they fixed some problems in Windows, in Microsoft Publisher, Word, Vizio, and Windows Essentials. So sort of your standard, run-of-the-mill Patch Tuesday, not as dramatic as some that we've seen.

One thing that I got a kick out of, though, was our friend Brian Krebs, who covered this Patch Tuesday as he always does. On his website he posted an open sort of side note to Microsoft. He just sort of, he said, "Dear Microsoft: Please stop asking people to install Silverlight every time they visit a Microsoft.com property. I realize that Silverlight is a Microsoft product, but it really is not needed to view information about security updates. In keeping with the principle of reducing the attack surface of an operating system, you should not be foisting additional software on visitors who are coming to you for information on how to fix bugs and vulnerabilities in Microsoft products that they already have installed."

So I thought that was - it's a very good point because I have had Microsoft saying, oh, like on a system that's recently set up, or one that you're curating carefully that doesn't have Silverlight installed. It's like, eh, no thank you.

IYAZ: As [indiscernible] in the chatroom is saying, you do need Silverlight for Netflix. And because you're going to be waiting a long time for those patches to download, you might want to watch a movie at the same time. So you should get Silverlight as soon as you can.

Steve: Yup. So also, as has been happening synchronized with Microsoft, Adobe updated Flash, Reader, and Acrobat. No real big news there. Flash fixes 13 vulnerabilities. Of course IE10 and Chrome will both update themselves automatically. You might need to restart the browser in order to get them to go and bring themselves current, depending. But basically just Flash Reader and Acrobat updated from Adobe.

I didn't check to see, after I restarted Firefox, that it had updated to 21. But I'm checking now. And, yup, sure enough, 21.0 just came out. This fixed a couple problems. There was a privilege escalation that Mozilla had been worrying about in their own maintenance service, which v21 of Firefox fixes. And then they also closed three critical holes, a couple which were remotely exploitable. So not huge and dramatic, but Mozilla's Firefox now moves to v21.

IYAZ: So you're telling me I should really update my Firefox 3 installation that's been sitting around because I haven't touched it since Firefox 3. I just leave it there in my applications folder because you might never know when you need it. Now it's up to 21. Okay. This went right past me.

Steve: Your go-to browser is what, then?

IYAZ: Chrome. I use Chrome.

Steve: Oh, you're okay if you're Chrome.

IYAZ: Almost exclusively. Almost.

Steve: Yeah, you and Leo are both Chrome people. I'm still - I love the add-ons that are available for Firefox, and I'm a major tab user. And I just like - I think I have, like, 87 tabs open right now.

IYAZ: I got so burned by Firefox and Mozilla constantly saying, yeah, we'll fix that memory leak problem. We'll fix that. We'll fix that. We'll fix that. After a while I just kind of got, yeah, sure, you're going to fix that. That's totally going to be fine. I'm not going to have my system overheating because Firefox or Mozilla promised me again. I guess the boy who cried wolf, or Firefox in this case, has happened.

Steve: Yeah, I understand that. They really did make an improvement in 17 was where - they began to beta their improved memory management in 14; 17 I think they pretty much nailed it. And frankly, I was just saying the other day that Google's Chrome really has become a hog of memory. I mean, you launch Chrome, and it's just, if you watch your memory consumption, it just squats down on a huge chunk of RAM. So I imagine they'll get to it. I like Chrome a lot. But I do wish they were continuing to fight back against that tendency to bloat it. So those are, however, Google's Chrome and Firefox are my two favorite browsers.

So in the news, I guess it was late last week, there was some interesting coverage about a report which was circulating of law enforcement having a seven-week wait for Apple to crack iPhone encryption. Now, that surprised everybody because we were assuming, I think it was when we went to iOS 4, that we knew that they deliberately took advantage of - wait a minute. Maybe it's iPhone 4. I'm getting my iOSes and my iPhones confused. But remember that they added hardware encryption in the phone hardware itself, which allows them then to do real-time decryption without any software overhead. And at that point, and we have covered this in detail explicitly in the past, it's possible to get your iPhone to be encrypted.

So it raised some concern. And the problem is we don't really know in exact detail - Apple has the technology. It's not completely open how it functions. We know that they have the keys to our storage in iCloud. That's well known. The presumption is, though, that a well-encrypted iPhone is uncrackable. Then we hear that there's a seven-week waiting list.

So to me it seems that it's probably a brute-force attack on the hardware. Certainly Apple has full knowledge and access to the phone hardware technology. So maybe there's a waiting list because it takes that long to brute-force access to the phone. Or, that is, it takes long enough that there's a huge demand from law enforcement to get into suspects' or captured iPhones and find out what they've got inside. But it's a little bit of a concern that Apple is there; although Apple, as other companies do, are complying with government requests for information. So I guess if Apple has a way of cracking it, then they'll say, well, we'll do what we can, but it may take a while.

And when I looked this morning, I saw the news that Syria had disappeared from the Internet once again. Two weeks ago they dropped off for almost a day. And I think they had just come back online when we were doing the podcast two weeks ago. Last I heard they had disappeared again. We heard two weeks ago that it was some sort of a fiber optic cable problem in Syria. It's like, well, okay. Leo wasn't buying that story. He felt it was clear that it was the Syrian government had some political reason for taking them off the 'Net. We don't know. But they're gone again. Or at least they were as of 7:00 a.m.

Pacific time this morning, 10:00 a.m. back on the East Coast.

IYAZ: I'm sorry I missed it. Was there any official explanation? Was it cable again? Or is this supposed to be government intervention once again?

Steve: I haven't checked for the last few hours, but they just - all we know is that Google services disappeared. Social networking services disappeared. There's something called - I think it's a Google service called Voice to Tweet or Speak to Tweet or something, which provides a means, maybe using phone technology, I think it might have been Speak to Tweet. Cell phone technology is then translated into tweets in order to still allow some access to Twitter, presumably, from inside a region which does not have Internet access. I did not have a chance to pursue that. But that apparently is something that Google did two weeks ago and was going to be doing again. So who knows if they're still off, and how long.

IYAZ: According to gmiola in the chatroom, he gave us a link saying that Syrian Internet is back up. Links to Syrian networks have been restored at 18:26 Damascus time, outage duration 8 hours and 25 minutes. And there's some charts over at Renesys.com/blog.

Steve: Okay, great.

IYAZ: Thank you for that in the chatroom.

Steve: Yup, so we're back. Or they're back. Okay, now, this was very disturbing. The "H" security guys, the H-Online, a well-known, U.K.-based security firm that we refer to from time to time, did some research to verify a report that they picked up on. The report was from someone saying that links they had sent, that is, this reporter had sent to someone else, were visited by Microsoft. So in order to verify that, the Heise Security group, they created some secure links, and they went to the trouble of embedding logon information in the links which they then sent through Skype chat to another user while monitoring the servers that those links referred to. And sure enough, a short time after that, an IP registered to Microsoft in Redmond accessed the resources behind those. And they were HTTPS secured links.

So this is sad. Apparently they asked Microsoft what was going on. Microsoft says, well, read the Terms & Conditions. We reserve the right to scan Skype chat for spam. And so apparently that's how they were justifying following links that were not related to spam activity, not phishing, just private HTTPS links sent in a Skype chat. Some server on Microsoft followed them and pulled the resources. And in this case the link contained all of the URL tail information required to authenticate a user for a secure logon, which Microsoft's query accomplished. So that's disturbing. That says...

IYAZ: Is there any positive look at this? Microsoft, they're trying to get away from spam in Skype. But if they're reading everything, that seems like there's - I'd think there would be a huge backlash based on this information being out there.

Steve: Oh, my god, they follow - yes. They're following links that people are sending to each other over Skype conversations. So first of all we know that it is - this notion, Skype originally had extremely good security. I mean, it was amazingly strong. And we know that it was also point to point. There was no ability to intercept Skype connections because it was direct user to user. Sometimes, when NAT traversal could not be accomplished, then you'd have to have a third-party relay, and that's what the Skype technology called it, a relay server, so that both of those users could access the relay, and it would relay the traffic. But that was typically just another user.

So what we now see is that, at least in the case of chatting, Microsoft is monitoring and reading everyone's chats and going so far as to follow links which have nothing to do with Microsoft, nothing to do with spam or phishing, they're just going there.

IYAZ: This sounds horrific. I mean, the things...

Steve: Really, really wrong.

IYAZ: Since Microsoft bought Skype, the infrastructure has changed so that we have a lot of this information going through Microsoft at this point. I wonder if a lot of this has to do with compliance with other countries that love to eavesdrop when it comes to Skype communications. And we've always heard the story of BlackBerry when it comes to countries constantly trying to get them to unencrypt things. And they're like, we can't do that. We just don't have the ability.

Steve: Right. Because the BlackBerry technology was well designed, and it was point to point. It was phone-to-phone encryption, and only those phones knew how to decrypt the session that they'd negotiated with each other. But obviously Microsoft has broken that, and we just - so the takeaway here is, first of all, this is important to know. And anyone should consider Skype charts are now being surveilled 100 percent by Microsoft. So you just can't use them for anything that you want to be secure.

There are some secure chat technologies, and people have been asking me about them. I think now it's time to go check those out and do some TNO analysis - that's an acronym we coined here, Trust No One - to verify that they are secure alternatives because certainly for chatting, at least, you need it. You and I are operating over Skype right now. It's a great service, the best that TWiT has found for solidly connecting people in a reliable fashion. But it certainly is no longer private.

IYAZ: Well, it's a good thing we're live streaming, as well. I don't think we have an expectation of privacy necessarily.

Steve: No.

IYAZ: But the chats, that just sounds crazy that that's happening.

Steve: And verified. I mean, the H-Online is a great group, and they have verified this is going on. And in fact you can probably google their piece because it was titled "Skype With Care: Microsoft Is Reading Everything You Write." And they verified it. Ugh.

Speaking of expectations of privacy, The New Yorker magazine just brought online an anonymous dead-drop system. The Verge covered the story. And it's interesting because just in the news also was the Associated Press's outrage over the admission by the Department of Justice - actually the DoJ confessed to this. They sent a letter to the AP saying that they had been, for several months - and I saw the word "20," and I saw a number "100" in different reports. So spying on at least 20 Associated Press reporters' telephone calls for several months last year, which really upset the Associated Press, you can imagine. Apparently this was regarded as a really over-broad surveillance of their organization. And Lord knows what information was discussed not relevant to any investigation that the Department of Justice had because they just threw this broad - they got a judge to issue the warrant which allowed them then to secretly tap the phones of these AP reporters.

But anyway, so it was interesting that, just while this was happening, The New Yorker

opens what they call "StrongBox." StrongBox is a Tor-based, secure, encrypted, anonymous dead-drop facility which allows people to share messages and files anonymously with writers and editors of The New Yorker magazine. It was actually designed by Aaron Swartz, who we'll all remember unfortunately committed suicide. And in fact it was ready to roll out late last year, but Aaron's death put sort of a pall on the project and halted it.

It's based on DeadDrop, which is open and free on GitHub. So although developers and users are cautioned that it's not turnkey at this point, it does take someone who really understands the system to set it up. It's based on three servers, two to do the work and a third one that monitors in real-time the operating security of the other two. And essentially somebody that wants to send something with absolute security, encryption, and guaranteed anonymity uses a client which accesses the Tor system to hide their identity.

When they essentially create this drop, they're given a random string which is their ID that allows them to then identify themselves as the submitter of the information, completely anonymously, so all The New Yorker sees is this information which they receive. They get it encrypted, and it is then decrypted on a - they get it as an encrypted file, and it is then decrypted on another machine not connected to any network. So, I mean, they really designed the security. Aaron used some very security-savvy people to design a provably secure, provably anonymous means of sending information to The New Yorker.

And of course this solves the problem, for example, here that the Associated Press is worried about. Of course the AP is, as would any news organization be, concerned that the government spying on them means that people will be afraid to have conversations with their reporters for fear that they're talking to Big Brother and Uncle Sam at the same time. So this system allows people to report things to The New Yorker knowing that they're remaining anonymous.

IYAZ: So things would remain absolutely secure, that if somebody blew the whistle on a company or some other activity, that no matter what, even if there was spying going on, you would never be able to, and the government would never be able to, backtrack to the originator.

Steve: Yes. Oh, and The New Yorker is able to have follow-on conversations that are also anonymous, all using this ID, which is the only means of someone identifying themselves. So they're completely off the grid and, as you say, able to provide information. And The New Yorker can't give the government anything it doesn't have. And it would have no idea who this was who submitted the information.

So it's interesting. The problem is there is very strong technology available now. So this is the kind of reaction that you would expect to see as a consequence of what people perceive as abuse by the government of their surveillance powers under the Patriot Act. It's like, okay, fine. If that's what's going to happen, we can roll out more technology to protect people who still want to be able to have a relationship with us and not worry about being compromised.

IYAZ: Is this something that a number of other organizations are going to adopt, as well? Or is this just The New Yorker for now?

Steve: I'll bet you we see everybody with a system like this. It'll get proven. Now The New Yorker has a means of soliciting this information in a way that people who want to submit things know is safe for them to do so. So that's a competitive advantage as a

news reporting agency. Absolutely, other organizations are going to say, hey, we want one, too. And there it is. It's called DeadDrop. It's on GitHub. You need some expertise to set it up, but the work is done. So I'll bet you we're going to see all news organizations at some point, of any size, that offer this kind of anonymous submission of files and information.

Okay, now, get a load of this. Oracle is changing their Java version numbering scheme, I kid you not, because there are too many updates to count using their current system.

IYAZ: Wait. Wait a second. There are too many updates? So instead of just trying to keep track of that, it's changed the number system?

Steve: Yes. Yeah, well, the problem was they had some scheme with the way they were allocating version numbers. But the need to increase the version numbers for updates, it sort of swamped the plan that they had for the way they were going to number things. So they've had to change their updating scheme because they're patching Java so often. So in the new system they have so-called "planned feature updates," which will now jump by 20s. So it'll go, like, Java Version 7 Update 20. Then it'll go to 40. Then it'll go to 60. And then their plan is that what they call "critical patch updates," or CPUs, those will be numbered by fives in between. So 25, 30, 35, and then 40 would be the next major planned feature updates. And that, then, that gives them room within the critical patch updates to have 6, 7, 8, 9 before they have a 10. So they've literally expanded the way that they number Java versions specifically to accommodate the fact that they are having to update it so often.

IYAZ: At some point they just have to call it Java Infinity, don't they?

Steve: Yeah.

IYAZ: Because it's going to constantly be updated. Just say latest, yes or no.

Steve: I thought it was interesting, too, to listen to some of the questions at Google I/O about the tension that now unfortunately exists with Java and Android on the Google side and Oracle's management of Java over on their side. So that's - but apparently no one's that concerned about it. They're convinced it's going to work itself out one way or the other, so...

IYAZ: The chatroom is making jokes of making it like an Apple style thing, like they should stop calling it iPad 3 or iPad 4. They should call it "The New Java."

Steve: Yes, "The Current Java," and don't worry about any of those other ones.

So yesterday, on what is today, today's the 15th, so it would have been May 14th, there was some sad news over in Bitcoin world. We've been following bitcoinage a lot recently just because it's been interesting and fun. Ars Technica reported that the Department of Homeland Security, our DHS, is alleging that Mt. Gox, which is the leading bitcoin exchange, is an unlicensed money exchanger dealing in crypto currency. And what happened was Mt. Gox had an account over at - do you pronounce it Dwolla? Dwolla? D-W-O-L-L-A.

IYAZ: I've heard Dwolla. Just, yeah.

Steve: Dwolla, which is a major - which is a licensed currency exchange that allows - it's sort of like a PayPal sort of organization that allows people to move money back and

forth between each other using Dwolla accounts that look very much like phone numbers. And that's your account number. Well, Mt. Gox had an account with Dwolla and a bunch of money there. And the Department of Homeland Security has seized all of Mt. Gox's money that was resident at Dwolla.

In the warrant, a special agent with something called Homeland Security Investigations, HSI, stated that there's probable cause to believe Mt. Gox is engaged in money transmitting, which is an official term, without a license. That's a crime, so says this agent, punishable by a fine or up to five years in prison. The warrant goes on to demand that Dwolla hand over the keys to account number 812-649-1010, which is owned by a Mt. Gox subsidiary. And quoting from the warrant, it says:

"Mt. Gox acts as a digital currency exchange where customers open accounts and fund the respective accounts with fiat currency, which is then exchanged into crypto-currency by Mt. Gox. The crypto-currency is known as 'bitcoin.' 'Fiat currency' simply refers to any money that a government has declared to be legal tender. The exchange is bidirectional and allows customers to also exchange bitcoins back into fiat currency, and then withdraw those funds. The exchange of fiat currency and bitcoins incurs a floating flat fee," I'm sorry, "a floating rate fee charged by Mt. Gox and is determined by the customer's aggregate amount of funds exchanged on a monthly basis."

So that was from the warrant. It remains to be seen what happens next. I was curious, and so I went over to see what had happened to bitcoin price. It did get pushed down from - it's been floating around about $120 in the last few days. It was pushed down, depressed to about $105, but has since rebounded nearly back to where it was. It's about $115 per bitcoin now. So it didn't - it wasn't considered a devastating blow to the bitcoin. We'll just have to see how this plays out and how it goes.

IYAZ: We were talking about this on today's Tech News Today, earlier this morning. And we were talking about the reach of the Department of Homeland Security, if they can even go out and do this, and why they'd bother to go this far to go to the - actually going up against Mt. Gox, why they're going after the exchanger instead of the actual person, just how hard it is to find out data on anybody who owns a bitcoin. You have to go all the way to the exchanger.

Steve: Well, and you would think this would be more of a Treasury Department thing, rather than Department of Homeland Security. And I thought that the Treasury Department just said that this was legal. But it must have been that it's legal from - I think that the paper, as I recall, it was about a month and a half ago, and that's one of the things that surged the bitcoin the way it did was Treasury said, specifically said that this kind of exchange was legal. Maybe, however, it was legal for users and not for money transmitters. And they're saying that Mt. Gox is a money transmitter.

And I do know that there was an agent who deliberately created evidence that DHS went after. That is, somebody set up an account with Mt. Gox, and an agent set up an account with Dwolla and then did move funds back and forth in order to generate a trail of evidence that was then used in order to issue this warrant and stomp on Mt. Gox. But obviously they're also confiscating funds, which is a concern. So anyway, we'll have our eye on this and see how it plays out.

Last week, in pure miscellany, and it was following from a tweet, I talked about how amazing hard drive magnets were. Those are the magnets that are in all hard drives now, which are the head-positioning magnets. In all hard drives there's a servo arm, or a head-mounting arm, which is pivoted on a bearing. The backside of that has a coil, which is energized. And the coil, the magnetic field from the coil, pushes against the magnetic

field being generated by these magnets. In order to minimize the amount of electrical power needed, you want the strongest fixed magnetic field possible. So as you can imagine, no expense has been spared by drive manufacturers creating the strongest magnets they know how to make. And oh, my goodness.

And so what I was saying last week was anybody decommissioning a hard drive, it's worth taking the lid off and taking it apart just for - even if you only do it once - to experiment with and play with the magnets that are inside. But you need to be careful because they are super strong.

So today we have a link, and I forgot to tweet this. I will tweet it as soon as we're done here so people can find it because - oh, wait, I did tweet it. I already tweeted it yesterday. So it's in twitter.com/sggrc. You can find the link in my Twitter feed, or you can also go to that archive of my tweets which is archived by Security Now! episode, and that's bit.ly/sggrc. So you can easily go back to Security Now! Episode 404 to find the tweet just before that. Anyway, the point is that the question was how many hard drive magnets are required to stick a young boy to the side of a steel shipping container? And the answer is 20.

IYAZ: Twenty.

Steve: And we have a picture of some guy who has his son stuck to a shipping container. Apparently under the son's clothes, his pants and his jacket, are 20 hard drive magnets. And then Dad lifted his son up and pressed him against the shipping container, and there he stayed.

IYAZ: So either this is the greatest dad in the world because he has a kid that wants to do an adventure, or this is the worst dad in the world, who is sticking his kid to boxes, giant metal boxes.

Steve: Actually, if you - yes. If you look through the guy's blog, it's clear that he's the greatest dad in the world [bit.ly/128TXYZ].

IYAZ: Good.

Steve: He's done some other things, like he's had all kinds of fun with cardboard boxes. And he's had his kids building forts and cutting holes and drawing on the outside and sticking their faces through the holes and all kinds of fun stuff. So this is definitely a neat dad. So the answer is 20 magnets will allow you to stick your son to a steel shipping container.

IYAZ: So, folks, if you've got a bunch of hard drives, I think there's a whole - there could be a whole cottage culture on this whole thing if you go Etsy and create these coats for children. Because I know there are plenty of parents out there who want to just take - I'm thinking about my two year old. Like, huh, maybe I could easily tell him to stay in one location. It'd be like a timeout jacket.

Steve: Actually many people said, hey this would be a great way to have timeout for your kid. Just lift him up and stick him against the wall.

IYAZ: But they might try to get timeouts because it's so much fun.

Steve: So I got a nice note from a listener of ours who specifically said "I want you to read this on Security Now!, Steve." The subject was YASSS, Y-A-S-S-S: Yet Another

SpinRite Success Story, from Christian Alexandrov, who's in Sofia City, Bulgaria. He said, "Hi, Steve and Leo. I want to share this story with Security Now! listeners and viewers. Usually I use SpinRite to help other people. This time I needed SpinRite to help me. This time SpinRite pulled my butt out of the fire," he wrote. "Thanks to you, Steve, I have a lot of RAM." And I thought, okay. He said, "A friend of mine was over, and we were having fun with my PC. Suddenly the PC froze; and, seconds after, we got the BSOD," the infamous Blue Screen of Death. He says, "I rebooted the PC. It did not boot. It gave me the BSOD saying 'Unmountable boot volume.'" Oops.

IYAZ: Oh, jeez.

Steve: "He challenged me, saying that if I fix it without the PC leaving the room, he will give me a brand new kit of 16GB of RAM - four modules, 4GB each, Kingston DDR3 133MHz RAM with eight-year warranty." He says, "If I lose the bet, I lose my PC." So Christian writes, "Bad bet. My butt was on fire because of the chance of losing my PC. My files? I have three redundant backups, updated every Sunday, all on various media, one offsite. I can get my data anytime, anyplace. Hard disks fail. This is why I have backups. But this is also why I have SpinRite.

"I took my case with CDs and booted the SpinRite 6 CD. I saw him worried. He was worried while looking at SpinRite's progress. And his worry increased when he saw DynaStat window popping out while SpinRite chews on a sector. After two hours of chewing, SpinRite gave me the green 'R' icon, fully recovering the sector, and quickly processed the rest of the hard drive. After SpinRite finished the task, I rebooted the PC.

"While the PC was booting successfully and fast to desktop, I was unpacking my new RAM. He asked me why I unpacked the RAM. I said, 'This was the bet.' While he verified that all works fine now, he just said, okay, fine, have it, it's yours. He left disappointed, and I left with a lot of RAM. Thank you, Steve, for this incredible program. And thank you, Steve and Leo, for this great podcast, in this case Iyaz. I wish best of luck to GRC.com and TWiT.tv from a happy SpinRite user." So Christian, thanks for sharing your story.

IYAZ: You don't get a cut of that, Steve. Do you get, like, 2GB of RAM sent to you because he used one of your programs? Kind of that Apple model of, hey, you used my thing, give me a piece.

Steve: Actually, the fact that I can share the story is all the reward I need.

IYAZ: Anyway, Steve, what's up next? We've got Facebook Monetization, is that right?

Steve: Yeah. The EFF, our friends who are really doing a great job of watching our back, the Electronic Foundation - wait.

IYAZ: The Electronic Frontier Foundation?

Steve: I can never get that right. It's, yeah, Frontier Foundation, Electronic Frontier Foundation, whose subtitle is "Defending Your Rights in the Digital World." They put out a really nicely assembled exposition that was titled "The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads." And I thought this was just - it's such good information, with enough technical meat that I thought it would be an interesting topic for the podcast, to give people sort of a look into how Facebook interacts with third-party data brokers. And we'll describe what those are. And it's not all bad news. I studied what they wrote. And I'm not horrified by what Facebook is...

IYAZ: There's a glowing endorsement that's going to be on the front page of Facebook: Steve is not horrified.

Steve: I'm not horrified.

IYAZ: Steve Gibson.

Steve: And normally I am horrified by these sorts of things. I'm not horrified in this case because Facebook, of course, is massive. With everybody now who's active in social networking circles, it's like - and you even see corporations saying "Go to our Facebook page." I was watching some little video about some wacky new car that gets 65 mpg on the freeway, and they're hoping to get off the ground. And they didn't say "Go to our website," they said "Go to our Facebook page." And it's like, well, okay, this has obviously happened.

The point is that Facebook has already been under scrutiny, so we know that they're going to go to some efforts to protect the privacy of their users. And we know that organizations like the EFF are going to be watching them closely, as are others. So they're trying to figure out how they can monetize their service while at the same time protecting the privacy of their users. So what I want to do is share this page with people, and we'll stop from time to time and discuss what we learn as we go along, Iyaz.

IYAZ: Okay.

Steve: So it starts saying, "Recently, we published a blog post that described how to opt out of seeing ads on Facebook targeted to you based on your" - okay, now, this is critical - "how to opt out of seeing ads on Facebook targeted to you based on your offline activities." So think about that for a minute. That means that it's not things you do online, but it's that your offline persona in the real world somehow is known to Facebook and/or Facebook advertisers, so that that's where the targeting happens.

"This post explained where these companies get their data, what information they share with Facebook, or what this means for your privacy. So get ready for the nitty-gritty details - who has your information, how they get it, and what they do with it. It's a lot of information, so we've organized it into a FAQ for convenience."

So the EFF poses this question: "What are data brokers, and how do they get my information?" EFF answers the question: "Data brokers are companies that trade information in people that trade in" - I'm sorry. "Data brokers are companies that trade in information on people - names, addresses, phone numbers, details of shopping habits, and personal data such as whether someone owns cats or is divorced. This information comes from easily accessible public data, such as data from the phone book, as well as from less accessible sources, such as when the, yes, the Division of Motor Vehicles sells information like your name, address, and the type of car you own.

"As Natasha Singer of The New York Times described in her portrait of data broker Acxiom" - and that's with a - they stuck a "C" in there, A-C-X-I-O-M - "last year [quoting The New York Times article], 'If you are an American adult, the odds are that [this Acxiom Corporation] knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams, and on and on.' Data brokers make money by selling access to this information."

So data brokers, their business is to build databases on actual people, on real-world physical people. And so their whole economic model is to make money selling access to

that. They have all this organized and online and accessible in some means.

IYAZ: This is intriguing. So these guys stand right in the middle between the DMV, I guess, and Facebook, something like that?

Steve: Well, we did have - we covered some time ago, I think it was in Florida, an instance of the DMV being caught, essentially, making revenue selling this arguably private government database information for money to third-party data brokers, to these sorts of organizations.

So the article continues: "Some companies deal specifically with regulated business purposes, such as helping employers run background checks on job applicants. Other data brokers sell or rent the data for marketing purposes. But details about where these companies get all of their data are still fuzzy. Rep. Edward Markey and Rep. Joe Barton" - one a Democrat and one a Republican - "and six other lawmakers sent open letters to data brokers last year demanding answers about their business practices. The letters asked the companies to 'provide a list of each entity, including private sources and government agencies and offices, that has provided data from or about consumers to you.'

"The companies gave vague responses. For example" - and I would call these "non-responses." Basically they said none of your business. For example, in its 30-page response, Acxiom, the company we were describing before, stated: "This question calls for Acxiom to provide information that would reveal business practices that are of a highly competitive nature. Acxiom cannot provide a list of each entity that has provided data from or about consumers to us." So basically they're refusing. Congress says what are you collecting, and the commercial organization says we're not going to tell you. The FTC has since opened an inquiry into data brokers because of concerns over privacy.

So then the next question in this FAQ is "Is there a government surveillance aspect to this?" To which EFF says: "There are government surveillance relationships to both data brokers and social networking sites that users should know. Many data brokers work closely with the government. For example, the FBI has been paying Atlanta-based ChoicePoint for access to its extensive database in order to screen for terrorist threats and for other purposes. And Acxiom worked with authorities after September 11th to track down 11 of the 19 hijackers and then continued to provide assistance to government agencies such as the TSA.

"We also know that the government looks to Facebook and other social media sites for a range of purposes, both for criminal investigations and much more. EFF and the Samuelson Law Clinic at UC Berkeley School of Law filed suit in December 2009 against a half-dozen government agencies for refusing to disclose their policies for using social networking sites. We found lots of evidence of the U.S. government using social media sites for data-gathering, including that the U.S. Citizenship and Immigration Services uses social media sites to evaluate citizenship requests, and that the Internal Revenue Service is poking around social networking sites to investigate taxpayers, and that the DEA is looking at social graphs of connected friends in order to map out associates of those sought in investigations."

So I guess this says that the government and the investigative arms of the government are not ignorant of and blind to the vast amount of information, I mean, I know that there's been lots of discussion about just how especially the younger generation just pours all of this information about their life into Facebook. And they're doing it just to share and to be connected and so forth. But all of the social graphs that can be generated from that are being data mined for purposes that the people sharing the

information probably didn't intend.

IYAZ: I mean, if they're publishing the stuff online and putting it out there publicly, they're probably not thinking of the repercussions of, like, mining this data. Because I've been thinking of this data, it's just a lot of people just in a vacuum. There's just their own information out there, not realizing that everything is linked together.

Steve: Yes.

IYAZ: Like when you click your friends or you're clicking your interests or whatever it may be, it's creating this image of you. And the fact that these government agencies get the information from the social networks without even breaking any laws, it's very simple. If it's public they can use it.

Steve: Yes. And we also know that, for example, employers have started to use all of the accounts that prospective employees have in order to do background research on individuals when they're considering them for employment.

So now the question: "What information is flowing between data brokers and Facebook?" EFF answers: "Facebook's new ad targeting program works with four data brokers: Acxiom," who we've been discussing, "Datalogix, Epsilon, and BlueKai. Companies who want to advertise on Facebook can use the data" - so we've got three entities. We have companies who want to advertise, and Facebook, and then these data aggregators who know about people in the real world. So "Companies who want to advertise on Facebook can use the data controlled by these data brokers to build custom groups and then show those groups targeted ads on Facebook.

"Certain technical steps, as well as Facebook policies, limit how much identifiable information flows between the data brokers and Facebook. Facebook did not explain the details in its recent note, saying only, 'the process is designed so that no personal information is exchanged between Facebook and marketers or the third parties those marketers work with.' A slightly more detailed, if somewhat outdated, explanation can be found in its description of Facebook Exchange.

"Here's how it works in practice for Acxiom, Epsilon and Datalogix," so the first three of these four data brokers, leaving BlueKai out for treatment in a second. "Under the new program, a company can approach a data broker, say Acxiom, and ask for a particular audience list, for example, a list of people interested in buying family cars." Now, it's a little creepy maybe, but Acxiom can actually answer that question. It's like, give me a list of all the people interested in buying family cars. Wow. Anyway, but apparently that's what Acxiom can do.

"Acxiom then would create a list of email addresses for everyone in their database interested in buying family cars." So Acxiom knows all of these people and has their email addresses. "Acxiom generates cryptographic hashes of those email addresses and sends those hashes to Facebook." So, and this is why, as I said, I'm less than horrified. I mean, there's still a lot - there's a lot about us that is known by these organizations, but there are nice barriers. There are walls that have been built to provide some protection.

"So Acxiom generates a population that fits a certain demographic that an advertiser wants, collects all the email addresses and hashes them, and provides Facebook with the hashes. Facebook, in turn, creates cryptographic hashes of the email address of every Facebook user." Okay. So Facebook maintains hashes of all of their users' email addresses.

"Wherever the hashes Facebook creates match the hashes Acxiom created, Facebook identifies that user as part of the target group. Any hashes that don't match are discarded, not used to form the audience. In this way, Facebook doesn't collect a list of email addresses of people who don't have accounts on Facebook."

So that's a good point. So Facebook is, I mean, notice that Facebook does know who these users are because they have the user accounts, they've got the users' email address, and they've got a hash of the email address. But the idea is that Acxiom will have, sort of in terms of a Venn diagram, Acxiom will also have lots of other email addresses that Facebook knows nothing about. And so these will be - so by both of them performing a hash of the email address, all they can do is say, oh, look, we know the email address and you know the email address. That's the only way the hashes can match. So no one is getting information about the other's email addresses that are not an overlap, outside of the Venn diagram overlap.

IYAZ: I mean, it sounds, like you were saying, not horrible. It does sound a bit sleazy.

Steve: Well, yeah. But we're going to be monetized, so this is how they're doing it. So "Any hashes that don't match are discarded, not used to form the audience. In this way, Facebook doesn't collect a list of email addresses of people who don't have accounts on Facebook." And of course, similarly, Acxiom gets no email addresses from Facebook either.

"Of course, it might be possible for Facebook" - it's a bit more than "might be possible," it absolutely is possible - "for Facebook to recover the email addresses using something like a brute-force attack." Well, that's not necessary because Facebook created the hash in the first place, and they know what hash is associated with which email address. And they say, however, "the company has a policy against engaging in such an attack." Well, if their policy says we won't brute force, that's useless because they don't need to brute force, as we just said. They created the hash, so they know what's on the other side.

Now, continuing, "The company that first requested the ad will then provide Facebook with a specific advertisement, for example, a family car advertisement, and Facebook will display the ad to the group that was created with Acxiom's data." That is, that data in the intersection of the Venn diagram. So what this achieves is you're a Facebook user, and even though none of your online behavior is indicative of an intent to purchase a car, by magic you're getting new car ads because some other company has been tracking you in other ways that they don't disclose to anyone, including the government, and they know that about you. And so they're able to arrange to show you an ad on Facebook that relates to something going on in your offline physical world.

"Facebook will likely be able to glean certain information about the user based on what is being advertised," obviously, "for example, ads showing baby clothes might indicate the individual has or is expecting young children, regardless of what the Facebook user posted on her profile," relating to young kids. "Facebook will also know whether the individual interacted with the advertisement." Which is a good point. Facebook knows if you click on the ad or do whatever the ad wants. "Facebook then provides the company with an aggregate report about how its ad performed" - obviously once shown to this target audience - "which might include information about how many people clicked on it, their locations, ages, genders, et cetera." Again, I'm sure anonymous, but still demographic profile to close that feedback loop because certainly Facebook has that information.

"While Facebook may be taking steps to limit identifiable data flowing back to the data brokers," and I would agree they are, "the result for users could be eerie. Users might

find themselves seeing advertisements that are based on actions they took in the real world as well as personal facts about their life and circumstances that they have been careful not to put on Facebook."

And then talking about just this fourth of the four data brokers that Facebook is known to be working with is BlueKai. Well, so, they're still - they're also in the business of aggregating information and selling their databases to Facebook and, of course, other companies, as well. So this is BlueKai, B-L-U-E-K-A-I. And we've heard about them before. They've been around.

But "For BlueKai it's an entirely different process. Specifically, BlueKai" - and I'm again reading from the EFF's great posting about this - "places tracking cookies on an individual's computer and uses those cookies to collect information about what pages that person visits." So this is old-school traditional DoubleClick.net-style tracking cookies. So that means BlueKai has relationships with other websites all over the Internet who have agreed to put a web beacon, a pixel, essentially, that refers to a BlueKai server. And that will carry a cookie which is uniform for a given user and allow BlueKai to track the user's movement across the Internet. So this is the whole third-party cookie problem that's well understood.

Continuing from the EFF, BlueKai "uses those cookies to collect information about what pages the person visits in order to show targeted advertisements. BlueKai shouldn't have any email addresses to share with Facebook." And it says, parens, "(In its privacy policy, BlueKai says that it is working to build a comprehensive online database 'with utmost attention and diligence to ensuring your anonymity and privacy.')" Uh-huh.

"In this case Facebook is using a process called 'cookie matching.' Here's how it works: Companies will start by approaching BlueKai and asking it to show an advertisement to individuals" - okay. So BlueKai is an advertiser in addition to a data aggregator, whereas the first three we talked about are only brokers. They sell the information, and that allows an advertiser to have the ad placed on Facebook to a demographic overlap that was obtained from the broker. BlueKai is an advertiser in the same way that DoubleClick is. And so it's BlueKai's ads which are scattered all over the Internet, which is allowing them to track individuals.

So here's how cookie matching works: "Companies will start by approaching BlueKai and asking it to show advertisements to individuals who, for example, visited the websites of hotels in San Francisco. When an individual logs into Facebook, Facebook uses an HTML pixel web bug with an HTTP redirect to allow Facebook and BlueKai to process the tracking cookies they have set on the user's computer. If a BlueKai tracking cookie is in place, the cookie will be used to look up what sort of sites were recently visited, what interests are associated with that account, and what kind of purchases BlueKai believes the user might be planning to make. BlueKai will then communicate to Facebook which audience to place the user in. The company that originally requested the ads will provide the advertisement to Facebook."

Okay. So essentially what's happening is BlueKai in this instance is not an advertiser on Facebook, yet they need a way of being a third-party cookie to Facebook's user. So Facebook hosts a BlueKai pixel which serves to allow BlueKai to obtain the information. This HTTP redirect, that's a means for Facebook to communicate to BlueKai and then back to Facebook to get this information from BlueKai, which then BlueKai uses to tie to all of the other websites that this Facebook user has visited. So that sort of - that's the means of breaching otherwise some separate spheres that there will be no communication between. So this is deliberate on Facebook's part in order to link the information. And then the advertiser provides the ad to Facebook, and then it inserts it

on the pages of those users that BlueKai says it would be relevant to.

So "As before, Facebook provides the company with an aggregate report about how an ad performed, which might include information about how many people clicked on it, their locations, ages, genders, et cetera. And, as with the other data brokers, Facebook would likely be able to glean certain information about the user based on what is being advertised," if it chose to look. And we really don't know one way or the other whether Facebook cares. "The end result for users is still somewhat disquieting: Websites you visited when you were not logged into Facebook will be used as the basis for showing advertisements on Facebook. This will happen whether you are logged into Facebook or not, and regardless of whether you consent to tracking or not."

So then the EFF asks, "What does opting out mean? In our prior post," the EFF writes, "we emphasized that the only way for individuals to get out of this program was to opt out. This means individually opting out on each of the data aggregators' websites of these affiliated data brokers," and EFF writes, "a Byzantine, multistep process. It also means that you will need to learn careful self-defense to protect yourself from BlueKai tracking you around the web. We recommend you use a tool such as Ghostery (now available on Firefox, Safari, Chrome, Opera and IE), or Abine's DoNotTrackMe (available in Firefox, Safari, Chrome and IE), or" - and, frankly, this is what I use - "AdBlockPlus with EasyPrivacy Lists." Which I find to be wonderful. "See more comprehensive instructions in our '4 Simple Changes to Stop Online Tracking'" posting, they say.

"Note that opting out of data brokers doesn't mean your data is actually removed from their lists. Instead, it just means your data is suppressed and hopefully won't be included in the data sent to Facebook. Please note also that going through the complex process of opting out of Acxiom, Datalogix, and Epsilon, as well as using a cookie-blocking tool to ward off BlueKai's trackers, may not be enough to protect your privacy from this targeted advertising program. There is nothing to prevent Facebook from engaging another data broker in this program in the future, in which case you'd have to opt out of that data broker, as well.

"You could attempt to opt out of every data broker," meaning on the Internet, they say, "but this is a Sisyphean task. It would be hard, or potentially impossible, to know if you managed to opt out of every single existing data broker, and quite difficult to know if those data brokers ever refreshed their data sets and added you back in. Furthermore, some data brokers may not offer any form of opt out. And even if you managed to get out of all the existing data brokers, newly formed brokers could always appear and list your information."

So finally they say, "Does Facebook have standards for companies who want to work for them?" And the answer, which is refreshing, is "Yes," and it just made those standards public. It's good that Facebook published a note explaining some of the minimum standards data brokers must achieve in order to work with Facebook, although some of those standards are inadequate. Here's what Facebook said:

"Inline Transparency. Users will be able to navigate using a dropdown menu to arrive at a page that identifies the company that was responsible for including them in the audience for the ad." Which is fantastic. I want to see that. "Facebook will also provide a centralized list of the third-party data brokers participating in the program.

"Control Over Ad Display. A user will be able to ask Facebook not to show a particular ad again, or not to show any ads from that company. Participating companies must also provide on their 'About this ad' page an opt-out of future targeting by that company."

IYAZ: But Steve, doesn't - by opting out and doing these measures, doesn't that give Facebook more information about the ads you want to see and not see?

Steve: Well, I mean, I guess I like the fact that, I mean, this is arduous. That's the problem, is all of this is opt-out rather than opt-in. But that's the way it's going to be. I don't think we're ever going to see this become an opt-in process, although the EFF would certainly like to see that. So yeah, you are, you're right. Certainly by any interaction you're providing Facebook with more information about yourself.

It may just be, I mean, I guess Facebook must be saying to users, look, if this ad upsets you for some reason, like, I mean, arguably there's some invasion of privacy here. I mean, because things you do in the real world are now being brought into Facebook, and Facebook knows what ads you are being shown. So in that process your information is being disclosed about you to Facebook by virtue of what ad, what group you are now part of.

So this is Facebook clearly trying to minimize that somewhat, after the fact, unfortunately. If you say "I never want to see that kind of ad again," then they're giving you some control over that, over essentially the upset that the presentation of this ad, which well could surprise people, could be creating by saying, okay, don't worry, you'll never see that ad again. And as you say, they are getting some information about their user.

EFF says, "Enhanced Disclosures" is also part of what Facebook has publicly said they're going to require. "Companies participating in the programs are supposed to expand their public knowledge centers so users can learn how data is collected and used." Well, okay, they're not telling the federal government when our Congressmen ask, so I guess we can hope they're going to tell random end users when we go to their websites. Good luck on that. "This includes explaining what types of information they collect and general information on what their policies are relating to the sharing of that data."

And "Data Access Tools. Facebook stated that each of its partners 'is working to develop'" - uh-huh - "tools that will help people see audience segment information that the partner has associated with them." That'll be a little disquieting. "The tools are also supposed to let users exercise control over that data. We saw the first example of this with Acxiom, which recently announced it would allow users the ability to access information about what categories of data are associated with them and make updates to those categories."

So the EFF says: "We think this is a good start, though we'd like to see stronger standards such as augmenting the Byzantine opt-out systems with respect to the clear Do-Not-Track opt-out signal, with a commitment to allow users to know what data a company has on them and what other entities have received that data. But publishing public standards was a big first step in the right direction. By creating a public policy for the minimum privacy standards companies must meet in order to work with it, Facebook incentivizes up-and-coming data brokers to improve their privacy practices in the hopes of one day earning a contract with Facebook."

And hear, hear. I completely agree with all of that. This is why it's like, okay, these are good things. And clearly Facebook is recognizing that in order for - they need to be perceived as not being an abuser of all the information which they're now aggregating and collecting and maintaining on their subscribers.

IYAZ: And with all the stories of Facebook and privacy concerns, the idea that Facebook would never want to lose a user, the fact is they're collecting this data that people voluntarily give them. And if they have to deal with any bad press about dealing with

companies that are monitoring your offline life, they are going to do their best to make sure that people believe that they can trust in Facebook.

Steve: Yeah. We're also seeing a trend in this direction. Look at some of the things we just learned that Google is doing, like analyzing all of the photos you took during a vacation and finding, I mean, like, literally doing photo analysis to spot the Eiffel Tower and to spot specific monuments and points of interest and recognizing those. That all goes into metadata about you. That's amazing. So we are really seeing deeper levels of data mining happening as the means for these companies to offer services that they think are valuable. And of course monetize their user bases, as well.

So EFF asks, "Will Facebook show me targeted ads on sites other than Facebook?" And the answer is, "Right now, Facebook displays ads when users are on Facebook, or sometimes when users are using Zynga and logged into Facebook. However, Facebook has reserved the right to show advertisements to users when they are not on Facebook." So all of this technology could follow you away from Facebook and create a longer reach, essentially, for Facebook. "Furthermore, Facebook is currently ignoring the Do-Not-Track signal. So while we are urging individuals to turn it on, just turning it on is not yet enough to get out of this targeted advertising program."

And, finally, "What should Facebook be doing differently? There's a lot Facebook should be doing differently," says the EFF, "when it comes to this new targeted advertisement program, such as stopping the program." [Laughter] Okay, good luck with that, EFF. "No. 2, making the program opt-in instead of opt-out." And we know that's never going to happen. Or, "Short of doing these things, Facebook has many ways it could address the privacy concerns of users. Here are a few suggestions:

"1. Respect Do Not Track. Facebook and data brokers should respect user wishes by committing to respect Do Not Track. This means not tracking users who transmit the DNT:1 signal" - which is a browser header we've talked about often on this podcast - "and interpreting that signal as an effective opt-out of this targeted advertising program.

"2. Facebook could use its market power to prompt participating data brokers to improve their practices." That's certainly true. "While Facebook doesn't have ultimate control over how these data brokers operate, it does have an extremely powerful role to play in the data economy. Through negotiating its contracts with data brokers, it can insist that these companies meet basic standards for respecting the privacy choices of users. For example, Facebook could require that all data brokers it works with provide users with a way of accessing their profiles and correcting inaccuracies and should ensure that a Do-Not-Track setting in the user's browser corresponds to opting out from tracking by that data broker. Facebook could also require each data broker to commit to not using data collected during the opt-out process" - which is sort of what you were referring to before, Iyaz - "for unrelated activities and to discard all unnecessary data once the opt-out is complete."

And, finally, "3. Facebook and data brokers could work together to create a single opt-out process. Anyone who is trying to opt out of this new targeted advertising program will see how complex it is. Users should not need to follow a complex process in order to opt out, and Facebook should use its place in the market to push for improvements. Facebook could set an important floor that could incentivize up-and-coming data brokers to improve their privacy practices in the hopes of one day earning a contract with Facebook." Which is a bit of a repeat of the text above. "Data brokers who are keen to prove themselves capable of self-regulation should welcome this major step forward for transparency and choice.

"In March of 2012," so a little over a year ago, "the Federal Trade Commission released its final report on digital consumer privacy issues, which included a recommendation that the data broker industry create a central website that would explain the access rights and other options, for example, opt-out choices available to consumers, and which would provide links to exercise these choices. EFF applauded this move but wished that the industry would go one step further and provide users with a single website through which users can opt out of having their data listed by any online data brokers," so a central clearinghouse, essentially, like the single Do Not Call list that we've had for telemarketers.

"Now is the time," says the EFF, "to make that a reality. Facebook could easily ask that companies who want to engage with them in showing advertisements agree to coordinate on such a hub website. Notably, the Privacy Rights Clearinghouse has already gotten things started with its Online Data Vendors List. Unfortunately, for now, the only advice we have for users is try to opt out of everything and stay vigilant."

So I'm glad we have the EFF. They pull this sort of information together, and they - I mean, knowledge is power. And so understanding what's going on and helping to publicize how this kind of tracking works is super useful.

IYAZ: I think people will be just shocked to know that there's all this offline data collection at all, the fact that these exist.

Steve: Yeah.

IYAZ: And then there's no actual statements by these companies how they're doing this. And then that they link to your online life, the fact that EFF is shining a light on it is fantastic, although I'm very curious if we'll ever get something as easy as a one-site opt-out process. That's be amazing. Then again, the Do Not Call list sounds insane, but it does exist. So maybe there's a chance.

Steve: Yeah. And what I think we're going to be seeing, I mean, now all the browsers support Do Not Track. The detractors say, yes, but it's optional. No one has to abide by it, et cetera. Well, yes, but it's a chicken and egg. You couldn't have legislation requiring its honoring until the browsers made it available. And there was that kerfuffle briefly about Apache not honoring it because there was one particular developer had a bug about Microsoft's IE10 he felt was like turning it on by default, even though in fact anyone setting up IE10 does see that, and it's well explained, like, what this means. Now that the browsers all have it, we might see some movement in Congress to simply require that it be honored if it's turned on. And ultimately I think that's what we're going to get.

IYAZ: Well, that was quite the educational episode of Security Now!. Every episode of Security Now! is like this. It's just it's explained to you simply. If I can understand it, I'm sure you guys are following along just fine, thanks to Steve. Steve, where can people find you on the web? Like maybe GRC.com?

Steve: GRC.com. And next week we will have a Q&A episode. And so our listeners pretty much probably have it pounded into their brain by now, but we are always getting new people, so GRC.com/feedback. You can go there to that page and send me a question about this or anything else that's on your mind. I go through the mailbag just before the podcast and pull out questions. And I imagine Leo will be back next week, so we'll go over that then.

IYAZ: He ought to be. Now, at GRC.com you actually have transcripts of each episode of Security Now!. That's right; right?

Steve: Right. As soon as you guys get this thing posted, I grab it and squeeze it down to our 16Kb version. I also have an archive of every podcast we've ever done, all 403. This one is 404. Elaine has a satellite link because she's somewhere out in the boonies, and so she is one of these bandwidth-constrained people that Leo talks about when he talks about our 16Kb version. So I immediately get that uploaded to GRC, and Elaine grabs that one to conserve her bandwidth and then does a transcription of the episode, which I typically post the next evening or sometimes Friday morning early, if Elaine ends up being up too late for me to get it that night.

IYAZ: You can also find show notes at TWiT.tv/sn. And normally we do the show on Wednesday at 11:00 a.m. Today was a special occasion because Google had their I/O presentation, pushing the show a little late. And Leo should be back next week. Thank you so much, Steve.

Steve: Hey, Iyaz, thanks for standing in. It was great. I'll see everybody next week.