Actionable intelligence to live a Free & Inspired Life

The Solari Report

March 14, 2023

Solution Series: Securing Your Privacy from Big Tech with Rob Braxman

Brought to you by Solari and Corey's Digs

James White: Hello, this is James White once again for the *Solution Series,* brought to you by *Solari.com* and CoreysDigs.com. We have a great show today, which is very timely. As always, I am joined by my cohost, Corey Lynn. Corey, it's always great to be with you.

Corey Lynn: It's great to be here. I'm looking forward to this one.

White: Yes, indeed. We have so many great guests here on *The Solution Series,* and we've had such great feedback. We do appreciate the people who tune in, read, and participate in this. We thank you for your participation and your support.

Today is going to be a good one, as they all are. We are talking about the surveillance society that you can see we are in. It's here now. We've talked about it for many years, and it seems like we are in it now. They seem to be managing the traffic lights and all of your smartphones, of course, and the facial recognition. We are going to cover all that today with our guest, Rob Braxman.

Let me give Rob a proper introduction: Rob is an Internet Privacy Guy on YouTube. He has been talking about privacy issues on social media for the last ten years. He is currently most active on YouTube, Rumble, and Odyssey. He is a public interest hacker and technologist. He uses his extensive knowledge of cyber security and technology to serve the public good.

Rob cares about privacy, and he can warn you of digital manipulation, disinformation, and mass surveillance. He is a successful software architect, and has had a career-building enterprise system in founding those companies. He is the creator of www.Brax.Me, a social media app for privacy enthusiasts, and he creates products and services for the purpose of defending our privacy.

Rob Braxman, thank you so much for joining us here today on the *Solution Series*.

Rob Braxman: I'm happy to be here.

White: It's great to have you.

If we can, a great place to start would be doing the 30,000-foot view, and then drill down into things. We know plenty about the problems, but we are here to talk about solutions.

Let's do a reset here: When did this begin? Computers came around in the 1980's, and smartphones came around later. Rob, when did this whole surveillance idea really get ramped up? Was it after 9/11? Was that the catalyzing event, along with the Patriot Act, that opened all that up? Or was that in the works before then, and those events helped? Or maybe that had nothing to do with it. I'll turn it over to you, Rob.

Braxman: When the internet first started, I already knew the internet was open, and you could see everything that went on in it. I was already worried about that and how it was going to be used. Of course, that was proven to be true.

You can say the internet side of things started in the 1990's when the internet started, and it's the complete structure of the internet that has allowed for this.

The government was already doing surveillance via the telephone system – the Public Switch Telephone Network (PSTN). But the internet side of things didn't start until the 1990's, and one of the things that was the earlier indicator of what might happen was email because email is wide open. It's a standard that is based on plain text, so anyone can read emails. I immediately said that this is going to be surveilled. Of course, Edward Snowden revealed that that was in fact happening and that AT&T was the primary infrastructure for doing that, even back then.

But it didn't turn into this personal surveillance thing because not everyone was on the internet in the 1990's. It did not turn into this personal surveillance issue until the phones came out. It started in 2007 when they realized, "Let's do this."

Google was founded by funding from three-letter agencies, so they already knew that was going to happen. So, the combination of the Google side from the internet, and they said, "We can go really personal here," and then they went to

the phone. Then in the last few years, that has gone to the extreme.

Lynn: I think that the phones are a great place to start. I get a large amount of emails every day, and the number one question that I get is, "What phones can we switch to?"

Many people will ask me about what to do about VPNs (virtual private network) or search engines or various things with their computers. We will get into some of that, but you know much more when it comes to the smartphones.

You talk about 'de-Googling' the phones and you talk about having different phone numbers, and even multiple phones or multiple SIM cards. I will let you expound on where you want to go with that and explain what can be done as far as protecting oneself through these wonderful smartphones. Even though I would like to tell everyone to just ditch their smartphones, I don't know how realistic that is.

If you want to start there, that would be great.

Braxman: The first issue requires some careful thought. Many, many people talk about being experts and offering solutions without really grasping the entire problem. I'm going to tell you the real problem because you can't just say, "Oh, it's a phone." It's not just a phone, and it's not just any phone. The issue has to do with something called 'cross-device tracking' or, to be specific, how you are identified by your phone.

This is the way the internet works now. That has changed; that is not the way it was. If you have a Google account, which probably 99% of the people do, and your Google account is on your iPhone and your android, the phone is clearly identified as being you.

The identification can go further because it could have your credit card from using the app stores and so on, but let's leave it at the identification side. The phone has a fixed identifier, and it is called the IMEI, which is a hardware identifier on the phone.

What Google realized was that, "We could take this surveillance thing further.

Instead of only saying that we are going to log into Google on your browser on your computer, we want to know exactly who you are. Yes, we tried those techniques like tracking your IP address and all of that, but we want to be even more specific."

So, in the last couple of years, they implemented where the Google ID is matched to all devices, and all the devices are now cross-tracked, called cross-device tracking. It verifies you by 2FA (two-factor authentication). So, the moment you go to Google, they say, "We require you to do two-factor authentication." That has been required heavily – two years for me now, and for some people it has only been a year. With a few exceptions, they have covered everyone with 2FA. That means that you use your phone as your identifier.

So, you are on your computer and on your phone, and the phone now matches. Now they say, "We know who you are because we can see that you are logged into the phone right now."

This is true of all phones. It is what I call 'normie phones' that are phones that have your standard operating system like IOS or Google android, and there is telemetry. It is sending out a ping to Google saying, "Yes, this phone with this IMEI is logged in with this Google ID." So, they always know where you are.

You can go onto your browser and hide your location and do whatever trick you want, but they know where the phone is. So, this is the thing that I am trying to explain to people: The main problem with the phone is identity. If you have a device that doesn't identify you, they could track all they want but the data is useless. But when they know you by name, they know exactly who you are, they know everything that you do, and they know every click on the internet. This is how Google analytics works; everything you do on the internet is matched to that Google ID as long as you have logged in at some point. You don't even have to be logged in now.

If you've logged in, it tracks everything that you do on the internet. That is now confirmed with the phone using that Google ID as the identifier. So, that is the main problem that I am trying to solve.

White: I know some people who have nefarious intentions with this type of

technology. How much of that do you think are people doing this not in your best interest, and how much of that are people who just want to make money? How much of this are people who want to track you for ads so they know where you are going and can put ads in front of your computer?

I've had conversations where something pops up on your phone or your computer based on what you've been talking about.

Do you think these people trying to do all of this tracking have money as the great motivation for them, or is it all about control? What are your thoughts on that?

Braxman: What you are talking about is what I've referred to as third-party tracking. So, the companies doing the advertising and so on are tracking you, but they are not the threat. They don't know exactly who you are; they only know what Google tells them. Google is trying to block them. They have something called FLoC. They changed that to Topics. Basically, it's a restriction so third parties can't know who you are, but Google does.

The reason this is a much bigger problem is that Google now uses secret information that only they have. Apple has it, too, but Google knows everyone, including Apple devices, because they know everything about you. Then they manipulate the internet to follow some secret agenda.

I've revealed this in a video showing how they used it to modify your search. So, you are searching for something, and they are trying to manipulate you by saying, "Oh, we know you're right-wing, so we are going to drop some things into your search so that you see other things." I believe that is a bigger threat than anything that is money-oriented. It's not only about that. I wish it were because then I wouldn't be in such a panic, but when somebody is trying to control me, then I worry.

Lynn: So how do we go about deGoogling a phone? What is the best phone to get?

Braxman: So now, we can go to the specifics because I set up the problem. The problem is that you need a phone without an identity. That is really the key

– a phone without an identity. How do you do that? Unfortunately, you cannot do that on a standard Google or android phone because they are built with trackers to track location constantly, and you cannot stop it. There is no permission necessary to stop Google or Apple from knowing the location of your phone. You can stop a third party from seeing the location, but you can never stop Google and Apple from tracking locations.

White: Even in a Faraday bag can't stop the signal?

Braxman: Yes, it can, but obviously, you are not using the phone when it's in the bag. They will track it once you take it out of the bag. So, then you lose the point of it.

The solution with the Google phone is that it replaces the code – the system apps that are tracking you like telemetry and so many of them. All of these telemetry apps cannot be removed; there is no way to stop them. They are hidden in the system, and you cannot remove them. So, the only way to remove them is to install a different operating system before they put that code in. Fortunately, we have that. It's called Android Open Source Project (AOSP). That is what we use as a base, and then we modify that.

So, Android Open Source Project does not have Google proprietary code because, obviously, they will not reveal that in open source. Fortunately for us, we can look at this Open Source Project, modify it, and use it as the basis for what we call a 'deGoogled' phone. Because there is no Google in it, there is no Google log-in. It never logs into Google, and there is no telemetry. It doesn't have a Play Store or any of that. There is no identity since you never logged in. So, Google can't identify the phone, and the thing that is interesting about the new androids is that the Android Open Source Project cannot read that IMEI (International Mobil Equipment Identity), which identifies that phone as yours. That is the key.

Google phones, in general, are based on AOSP, so that is the main gist of it.

Lynn: You have a phone that you sell, correct?

Braxman: Right.

Lynn: I've seen others on the market. People, like me, are good with tech, but I'm not a techie; I don't know the back-end information the way you do.

I've seen others on the market, and they will say they are de-Googled, but how do you know that?

I want you to briefly talk about your phone. You don't have to compare it to other phones, but the important thing is that once they have a phone like this, don't log into Google or start downloading social media apps.

Braxman: I wouldn't worry about that if you have the right phone. You cannot 'screw it up'.

Lynn: That is good to know.

Braxman: That is the interesting part; you cannot 'screw it up'. I will explain that later.

So, Googling is based on Android Open Source Project, and there are many people who do it. The most popular one – and the one that I use for phones that are not mine – is assuming I'm using a Google Pixel phone. This phone is made by Google, and fortunately, because it's made by Google, it is completely compatible with Android Open Source Project.

The most popular operating system for deGoogling is called LineageOS. That is what I use when people ask me and my company to deGoogle their phones; we use LineageOS. That is the most popular, and the reason is that it was first. It is also used with more phone models. If you want to check if your phone model works, you can go to www.LineageOS.org and see if your phone is supported. If it is, you can deGoogle it based on whatever restrictions they have on it.

That is one way. I made my own phone, which is running braXos.

White: You made your own phone? That is brilliant!

Braxman: Yes, and we have been selling this phone. We also sell the Pixels

running LineageOS. It is less expensive than the Google Pixels because we don't have the overhead of Google. We have our own OS, and because we can control the OS better than we have with Lineage OS (because it's not ours; it is some volunteers doing it), we can control this. We have a deft team that works on the OS for this. So, we have better control of the phone.

Some of the problems you will find if you say, "I'm just going to go with LineageOS," is updating it; that is problem number one. The second issue is if the phone has all the features. Typically, when you use LineageOS, we have to tweak it at our store before you can use it because it doesn't come with anything; there is no App Store. So if you do a reset, you are 'stuck'.

With the one we made, it doesn't have those problems because we already preconfigured it with certain apps already installed. So, it's much easier to use.,

Those are two options. There are other OS's that are based on Android Open Source Project that are equally acceptable for deGoogling. There are too many of them to mention. They are okay, and there are no problems with that except that you have to do it yourself. If you can do that, that is fine.

My push is that you don't have to buy my phone or my service; you can do it yourself. It is more important that we all deGoogle.

White: Does your camera work on your phones and the Bluetooth and the Wi-Fi?

Braxman: Everything is normal except for the one thing that we do: We block the Wi-Fi triangulation that spots your indoor location. That is intentionally disabled on this. So, it can't actually spot your location unless you give it permission. It works on any other phone that is not braXos. It is possible to get your location even if you didn't give it permission because Google and Apple can do Wi-Fi triangulation in Wi-Fi scanning and all these little tricks they do.

Lynn: So, if someone wanted to download social media apps or something to that effect, you are saying that is safe?

Braxman: Let's cover this because that is very important.

Lynn: Yes, because they have the privacy and terms and all that.

Braxman: You're right. This is very important, and this is a practical thing. Believe it or not, when you use a deGoogled phone, especially something like braXos, which is preconfigured with what apps to work with and an app store, we don't use a Google Play Store; we use another store called F-Droid. So, there is a substitute store.

When you do this on a phone, if the app can be downloaded, you can try it and see if it works. You can even download Facebook and it will work. It will actually give you a message saying, "It won't work," but it does work. Instagram also works. Those two are the most dangerous social media apps ever. Anything to do with Facebook is the most dangerous social media app.

Believe it or not, you can run TikTok and Snapchat and all that; it works. On my phone, I have Kindle and we preinstalled Waze on it. Waze is owned by Google, but it actually works. I even have a Tesla app. I have Spotify and Netflix and all that because it all works fine.

You are not giving up technology when you deGoogle a phone. What you lose is you can't watch YouTube on YouTube; you have to use the browser if you want to do that. You can do things on the browser.

As far as apps, you cannot install anything Google. You cannot install Gmail or Google Drive. Nothing Google will work; it will fail. You have to use a substitute for Google Earth. So, anything with Google has been substituted.

As far as what the actual danger is, the main issue is identity. Because the IMEI or the identifier that identifies your specific phone is not accessible because there is no Google app there to spot it, there is no way for a third-party app that is based on permissions, like TikTok, which has been touted as being very dangerous, to read the IMEI like Google can. It can't see anything. It doesn't even know the model of the phone. So, it can't find the phone number. It can't see any of the things that Google or Apple/iPhone can.

A third-party app of any sort – no matter which one it is – cannot do it on a deGoogled phone. Permissions on location are quite specific. If you block permission for location, the app doesn't get location, whereas with Google, you can say, "I'm going to block location," and they can still get it.

A phone like this is very hard to 'screw up' because, how can you 'screw it' up? Let's assume you are using Facebook. Facebook has other tricks 'up their sleeve' to spot you. Let's pick TikTok again because that is rather well-known as a bad Chinese app. What can TikTok do? TikTok cannot even see all the other apps that are running on your phone. They don't know what else is on your phone; they just know their own content. They can't get your location if you are blocking it. They cannot get your identity. They don't even know who you are.

If you create a fake identity on social media – and this applies to all social media – I don't understand how it can be a threat. That is very important. Control your identity from your log-ins and two-factor authentication. A deGoogled phone does not have the connection that allows cross-device tracking. So, it's almost a perfect solution.

Once you have a deGoogled phone, you disappear from Google; you just disappear.

White: That's fantastic! What about Apple? It sounds as if you have an Apple phone, you are just about out of luck, right?

Braxman: Yes, unfortunately, I do not have a solution for Apple. Apple, even with your phone off, turns into an AirTag, and it is tracking your location 24/7 no matter what you do as long as there is a trickle of a charge on that phone.

Lynn: What about VPNs while surfing the internet? What is your opinion on VPN?

Braxman: That is very important. I have a trio of things that I consider to be key to privacy. The number one thing is the deGoogled phone. So, it's not having a normie phone but a protected phone like a deGoogled phone of some sort. That is number one.

Number two is a VPN. These are all used to identify you. Everything that I talk about is related to identity. A VPN will prevent someone from identifying a specific IP address. The purpose of a VPN is to group you so there are a number of you with the same VPN, and they don't point to your home with your IP address, so therefore, there is no way to specifically identify you. I will tell you this, though, "If you are using cell data, there is no IP address to worry about, so that is kind of like being on a VPN. If you are using Starlink, it is also like a VPN because it doesn't have a fixed IP address since your unit is in the sky. That is the IP address that they see – whatever the satellite connects to; they don't see the IP address of your home router. So those are equivalent to VPN."

The third protection item in my trio, which is basic and part of the main protection scheme for privacy, is called browser isolation. This is part of the identity problem that I talk about. Google has you identified by a Google ID. If you log into Chrome with your Google ID, everything that you do on the internet is now connected to the phone and everything that you do on the internet. I don't care what website you go to; it will know what you do on that website. This is frustrating because there is no way to stop this.

I created this procedure seven years ago when I first realized this problem. I was talking about this, and I came up with my own description of it. I call it 'browser isolation'. No one has ever used this term in the way I've used it. I somewhat invented it. The scheme of this is very simple: You use multiple browsers, and you leave Chrome as 'Google', but do not go to any other website that is not owned by Google on Chrome; Chrome is for Google only.

What is the effect of this? The Google ID cannot cross browsers. The Google ID is then isolated to whatever you are doing on Google, which they already know, and nothing happens. But if you go to Amazon, go there on a different browser.

I have three or four browsers on every computer that I use. I set aside one for the other. So, let's say that you want to protect yourself. You go to some other platform that is not owned by Google. You keep it separate by having a different browser for it, which is called browser isolation.

That stops the Google ID (identity) from crossing into whatever else you are doing on some other platform. This trio of things is quite essential to making sure that what you do on the internet is not tied to a specific identity; it's just random noise on the internet. This is really the key to protecting it. That's it.

Lynn: Going back to the browsers, I use multiple browsers as well. Give me an example of something that you are going to do on the internet where you will bounce from one browser to a different browser to a different browser.

Braxman: I believe it's quite simple. If it's not Google, you can use one browser for everything non-Google. I do that. The one I use most often, because I use Linux, is Chromium. Chromium is actually the basis for Chrome; it's the basis for Edge; it's the basis for Brave; it's the basis for many other browsers. But when I go on Chromium, I can do anything, but I never log into Google on that browser.

Once you log into Google on that browser, it keeps a cookie there that identifies you and it is browser fingerprinting, and then you are tracked and everything that you do there will now be found by Google Analytics, and it will connect everything that you do.

This is the important part: Almost 99% of all websites around the world have Google Analytics. What is Google Analytics? It's the code that Google gives to you. They say, "Put this on your website so we can track your traffic and give you ads and put you in our search engine."

Everyone said, "I want to be in the search engine, so I'm going to put Google Analytics on there." So, almost every website has Google Analytics built in.

The Google Analytics detects your Google ID. If you don't know this in the advertising world, you can actually spot people and say, "This person is interested in art photography and food and all that. We know it from the Google ID."

So, if you do not have a Google ID, they cannot collect this information and put it into your record. So, by leaving every other website to its own browser without a Google ID, there is no way to collect that information and put it in

any bucket.

On the Google side of things, assume you are using Chrome. You are on YouTube, and YouTube already knows what you are doing because you're on Google. Google already reads your Gmails and knows everything that you are doing in Gmail. There are no secrets there. That is a different problem that you need to investigate, but that is not part of the hardware set-up that we are talking about here. I'm giving you the basis for the tools you need to stay protected.

There are procedures that you have to apply to all of this if you want to be serious about it, but even what I've already said is enough. This will probably solve 80% of the problems.

Lynn: I have two quick questions: Going back to the phone, what about the service provider? Let's say that I'm going to buy a de-Googled phone. Now I need to determine if I want AT&T or Verizon. What service am I going to get? Is the service provider itself going to be able to track anything or pass that information along, and those types of thing?

Braxman: That is a very good question. This is why there has to be a separation of threats. In my line of work, cyber security, you have to identify a threat model. Who is a threat to you? You mentioned advertisers and so on. I don't think they are that much of a threat. The threat is actually big tech. Which big tech? Carriers are big tech and Google and Apple and Microsoft and Yahoo and so on are another type of big tech. So, there are two kinds of segregated big tech that have a serious impact on you, and both of those groups of big tech can do mass surveillance – the carrier side and the social media platforms.

The problem is that the phone side of things (the carriers) is tied to the government. The specific threat of carriers relates to the CALEA (Communications Assistance for Law Enforcement Act). So, everything that you do on the home network is called the PSTN (Public Switch Telephone Network). Everything you do on the phone network is surveilled and collected and recorded. It goes into the FBI-DCIS database – every call, every text, everything. So, there is no real way to hide that; that is just how it is.

You have to think about when you want to be on the PSTN since there are options now. You can use apps like Signal and Session and even Brax.Me (my own app). You can use these to obfuscate your communication so you don't have to be tracked with mass surveillance.

Given there is that option, we have a solution: The thing is that you cannot stop the phone companies from surveilling anything that you do because it's part of the government system. It's actually linked in hardware.

CALEA was passed during the Clinton Administration, and they have integrated that, by law, into the hardware. So, in every country anyone can tap you at will. There is no need for any physical wire-tapping; they just go into the software and log in and tap you. Then they have a record of all your texts in the FBI database.

White: Isn't that a tremendous violation of our Constitutional rights? Or has that already been adjudicated?

Braxman: That is a law; they passed the law saying, "We are going to do this."

White: What a joke!

Braxman: It's quite crazy, isn't it? Snowden revealed the PRISM (Planning Tool for Resource Integration, Synchronization, and Management) program, which is exactly the type of tracking I'm talking about, but now they've made it easier. So, PRISM allows them to spy on all of your traffic.

There is a law that says they cannot record your calls unless there is a warrant, but they have all the mainframe data. So, they already know who you called, what time you called them, and how much time was spent on the phone, and who the parties are on the other phone numbers, and on and on. They can capture the entire text. So, texting is more dangerous than a phone call because, with a text, they actually see what you said. There is no law that stops them from recording a text. So they record every text.

There is no protection here; it's just the way it is. So, the solution is to leave the

phone network where you can. Don't use texting or phones for normal use.

You can communicate with your friends using Signal. By doing so, you disappear from the phone network, and they can't track you.

Lynn: Do you prefer Signal over Telegram?

Braxman: I do not use Telegram, and I do not prefer Signal; I prefer Session.

Lynn: I'm not familiar with Session.

Braxman: I made a new video on YouTube on Session. It's far superior if you want privacy. Signal requires a phone number. Session doesn't require anything; Session is a step above. All of the network traffic occurs in what is called the 'dark net'. They cannot actually watch the traffic of Session even if they tried to look at it from some 'three-letter agency' level because it's happening on the dark net, similar to Tor. They have their own dark net that is not Tor.

Lynn: I will have to check that one out.

Braxman: That is my new video, and that is my preferred way. You can use Signal for people you already know because they know your phone number.

If somebody doesn't know my phone number in advance, I'm not going to talk to you through Signal because I have to give you my phone number. But on Session, I don't need a phone number; I just connect.

Lynn: That's 'awesome'! Using two factor authentication, do you deem that as a good thing or a bad thing? Should a person use an email as opposed to a phone number?

Braxman: You don't have a choice; they don't give you a choice. I'll tell you what you do; There's no choice with 2FA. Do you need 2FA? 2FA, as originally intended, is a good thing. I made many videos showing how it's a bad thing, but it's a bad thing because it was abused by certain parties.

When your bank says, "I need 2FA," you say, "Okay," to the bank because that is your money. When somebody like Twitter says, "I need 2FA," you start to wonder, "Why does Twitter need my 2FA? How important is that? Why does Facebook need my 2FA? Why does Google need my 2FA? Why are they so restrictive with it?"

It's a problem because Google and Facebook have created this 2FA as a way to piggyback their surveillance. I discussed this before when we were talking about cross-device tracking. They're not only using 2FA for what it is intended for, which is two-factor authentication; they are saying, "We are going to go beyond that."

There are other ways to do two-factor authentication without giving a phone number, but they want to go beyond that and track you. So, Google and Facebook 2FA are extremely dangerous because they've gone beyond the normal 2FA reason. They are using it for cross-device tracking. They want to find out your specific device ID so they know what phone you are using and identify you by the phone.

In fact, on Google, you can do two-factor authentication without a phone number as long as you assign a normal phone, like an iPhone, where they have the identity of the phone and they have the location at all times on that phone. Then they say, "Okay, you don't have to use the number."

White: There is no way to opt out of this, right? There is no way to say, "I don't want you surveilling me."

I've heard that you can turn off your location services, but that doesn't even matter; they will track you anyway. So, is there any way that you can legally opt out of this and say, "I don't want to be surveilled"? Or, because you choose these terms and conditions when you log into your phone, they are legally able to do that. Is that accurate?

Braxman: That is correct. There is no way out with this. My solution is to use the BraX2 phone that I sell, which has two SIMs. So, my second SIM is a two-factor authentication SIM.

The important thing is that the second phone number used for two-factor authentication must not be known by your friends; that is the important part. What they do to track you is say, "What is your phone number?" Then they cross-check it against contact-listed people or people on Gmail or LinkedIn or Facebook or whatever. Then they can cross-check and find your real name and phone number. This is a very common technique. They can find you if you use the same phone number. They can say, "I know exactly who you are because we can search contact lists and find out what your phone number is."

The solution is, if you use a second SIM card or a second phone like a spare phone that you don't use much and that you leave off, use that for two-factor authentication.

In this case, I have a second SIM card. So, if I need to do two-factor authentication, and Google likes to do this because I have a YouTube account, then it goes to the second SIM card, and the phone number is not known to anyone. In fact, I don't even know my own second phone number because I keep changing it, and they cannot match it to anything.

That is what I use.

Lynn: So, the phone that you built has two SIM cards in it. I like that.

Braxman: Every phone that I will release will have two SIM card slots.

White: That's brilliant! That's some rather good thinking! I didn't even know that you could put two SIM cards in a phone.

Braxman: Practically no US phone has it, and iPhones are eliminating SIM cards and going to eSIM, which is a really bad idea for privacy.

So, I recommend you use two SIMs. You might think, "That's kind-of expensive to have two SIMs and two separate plans." Well, since the second number is going to be low-volume use, and it's only going to be used for texting, I've found a plan that can handle it, and I'm paying $60 a year for that. That is what I'm using for my 2FA.

White: That's 'crazy cheap'!

Braxman: So, it's $60 a year (or $5 a month), and I have the security of knowing that my phone number is not part of the Google tracking or Facebook tracking mechanism.

Lynn: Are you doing it as a forward? Are you setting up numbers outside of it and doing it as a forward, or is it a direct number that is just rolling over?

Braxman: No, it is separate. Otherwise, Google will not let you. It has to be an actual phone number. You can change your phone number if you feel like you've been compromised in some way. It's only a SIM card; change the SIM card. Go to your carrier and say, "Change my phone number."

My old policy used to be that I would change my phone number as often as once a month, but I don't think that is necessary. I was being a bit extreme since nobody knows the number. But if you feel like the number is now known because you accidentally gave it away to somebody, then you change the phone number.

White: Are there any advantages, security-wise, to turn your Wi-Fi off at night? Is there any security to turn your phones off at night? Should you turn your computers off? Or are we way beyond worrying about that now?

Braxman: I don't know what that will do. When you turn them back on, that queues up or 'caches' all your location information and everything that you do. When you turn the phone on, all of that information gets sent to them then. So, I'm not sure that is actually doing anything.

Many people do turn off their Wi-Fi at night because they feel like they are getting frequency effects. That isn't my deal, so I don't worry about it.

The only one I would worry about is the iPhone. Since I don't use my iPhone for anything except for 2FA, it is kept in a Faraday bag, and it is in there 99.99% of the time unless I need an emergency 2FA. It's only for emergency 2FA's, otherwise, I don't use it.

Lynn: What is your preference or recommendation on search engines? I hear people go back and forth as far as Firefox or Brave. What search engines do you recommend? Do you think it's not even relevant to how they are gathering information?

Braxman: It's very relevant because the Google ID is connected also. If you do browser isolation, it cuts down some of that. But if you don't do browser isolation, obviously everything that you do searching on Google is part of that record. So even on Chrome on the browser isolation that I mentioned, I do not use 'Google search' on that. I make sure that Google is turned off.

My preferred one is Startpage. You can find it at www.Startpage.com. The advantage of Startpage is that Startpage uses Google search, but it takes off your identity. This goes back to the identity problem, so that is my preferred one to use.

Some people use DuckDuckGo, and more recently Brave. You can use Brave; I have no problem with Brave. The search results on Startpage are better, so I would prefer that for that reason, but DuckDuckGo started to get political, and so did Firefox. They started to do censorship, and that really bothered me. For that reason, I would not use DuckDuckGo since last year they began to censor.

If I am going to get censored results, just like Google manipulates my results, then it's goodbye.

White: What about Opera? Opera has a built-in firewall apparently. You're not a fan of that?

Braxman No. Opera is owned by the Chinese. It's not actually a VPN. What they offer on Opera is called a 'proxy'. That means they can spy on you on the proxy. So, everything that you do on Opera will go to the proxy, and they can go see what you're doing and what websites you are visiting, and they can use that information. So I wouldn't use Opera.

I only have one browser that I tell people never, ever to use, and that is Opera.

Lynn: What about storage? Many people use Google Drive, of course, but

some people are also hooked into the cloud – whether it's through their phones or their computers; They use it for storage.
Is there anything that you recommend outside of that for people to use instead?

Braxman: Yes. In fact, I am making a video on it in next month. I don't have the answer to give you right now because I'm in the process of testing it, but there is a hardware solution where you can reach your home cloud. Your server and the cloud can be reached at your home, and using your phone you can do that. That is what I am suggesting as a hardware solution, but I have to test it out before I start saying, "This is going to be a good solution."

It's not a sponsored video; it's something that I can test out. Then once I've found what seems to work, then I will have that offered as a solution.

The alternative solution for somebody more techie is to install your own cloud in the cloud, which is obviously a more expensive solution since you have to have a cloud account using NexCloud. If you are a techie, you can set up your own NexCloud server.

White: What about ProtonMail? That is a secure offshore server where you can send mail out, and it's not processed in the United States. It is supposed to be secure. Do you have any thoughts on ProtonMail?

Braxman: Yes, definitely. I have a very hated video on ProtonMail because I said, "Don't use ProtonMail."

If you understand how email works; email is a big topic for me. I make many videos on it because I am very experienced with email. I have made my own email servers and I have had email clients since the 1990's. So I am very skilled with this, and I understand exactly how to do this.

I made a product somewhat like ProtonMail which caused me to understand that I shouldn't be doing this. This is why I stopped doing it: I watched the traffic, and said, "Oh my gosh! We can't do this."

If you are using ProtonMail, you have to understand that 99.99% of your mail is not encrypted. Why? Because you are talking to Gmail and Yahoo and all of

them. You are talking to other people; you are not talking to ProtonMail people. The encryption, even with my own product, is only intra-domain. So, in my case, it was Braxmail to Braxmail. Yes, that is encrypted, but as you leave that, then it's not encrypted.

So, what is the point of going to ProtonMail if ProtonMail can read everything that goes through? What are you actually gaining?

What you gain is a negative gain, so it is actually a loss. You have now announced to people that you are using ProtonMail.com or Tutanota, which is equivalent, that you have something to hide. Why would you need to do that when your mail is open anyway?

Since there is no way to encrypt normal mail, which is 99.99% of what you do, I don't need that solution; I just need to make sure that my email provider is not using my data for analysis like Google does. So I offer Braxmail, which is my product. Or you can use any paid email service. I don't really care who it is, as long as it's not part of the Google or Microsoft or big tech companies that actually collect your data.

In my case, the difference in the Braxmail that I make, which is important because of the IP address problem, is that when you send out email, your IP address is on the email. I don't know if you know that, but every email that you send out identifies you. The solution is to have a product that removes identifiers from the email, which Braxmail does. That is the only thing I need to do. The email itself is already clearly spied on. I mentioned that they've been spying on emails since the 1990's.

White: What about Pretty Good Privacy (PGP) where you encrypt it on one end and then you send the encryption key? Is that still a solid way to encrypt messages via email that you want to keep secure?

Braxman: Yes, but it only encrypts the body; it doesn't encrypt the header or the title or the meta-data that says, "You communicate with x."

Let's assume you are a whistleblower. During Snowden's time, he didn't have an option. Maybe he had an option, but not something that most people used.

How does he send out a whistleblower message to somebody without metadata?; he had metadata. All he encrypted was the body. So, it could be clear that he probably had an IP address, but somebody attributed to him contacting Greenwald at *Intercept* or whatever. So that was an issue.

It's called PGP encryption, which is obviously useful when you want to obscure the body, such as financial information, but it doesn't obscure who you are talking to. The metadata exists, and so that is not a good idea.

Obviously, the solution is to not use email.

Lynn: That was my next question about metadata.

In documents or photos, if someone is uploading a photo to social media or they are sharing documents or PDFs, what do you recommend for ways of stripping the metadata out of images or documents? You just covered emails.

Braxman: Let's say that you are using a deGoogled phone where you know that you can block a real location. All you have to do is not give location permission to the photo app, and it will not have location information on there. So that is the easiest way. Then there are many, many apps out there that can also do this. In fact, Brax.Me does this. You upload a photo to Brax.Me and download it, and it strips out the metadata. But you don't normally have to do that if you stop the permissions for location ever going into your photos.

It doesn't matter what the phone is. Even if you're using an iPhone or a Google android, never give location permissions to the photo and gallery app. That will stop that piece of metadata.

There is not an actual piece of metadata that is a PDF file; the metadata is part of the format for a photo, but the PDF has to have the original metadata when you create the PDF (like who made it, etc.). That will stay with it, just like with any Microsoft Office document. It has the timestamp when it was created. The only way to remove that is to take the data and cut and paste it into a new document.

White: I have one final question for you because I know we are getting close

to the end. What about a burner phone? I'm talking about the burner phones that you can buy at Walmart for $40 and pay $30 for a month's subscription. Do they still track you with that? Is that something that is a quick fix if you are on the road and you are a whistleblower and want to meet with somebody privately? How is that as far as privacy is concerned?

Braxman: The questions that you have are almost like all of the videos on my channel. I had a video demonstrating this. It was called 'The Jason Bourne Video'.

The idea of the video was that you are trying to escape the government, so what do you do?; you are escaping. I show every mistake you can possibly make so that you can be spotted. At the end of the video, you are spotted anyway, but you can delay it for a while if you know all of the techniques. So it's not perfect. Jason Bourne could not escape, so he had to fight his way out at the end.

That takes some fairly advanced thinking to understand this, but the moment that you use a phone, even a burner phone, the thing that most people do not understand is they don't track you with a burner phone. They don't know who you are – at least not initially. They can find this out later on because they know where you bought the phone. So, they can't track you when you use the burner phone, but they can track who you call.

So if you called your wife, and if someone was listening to you, they're not going to track you because they don't know who you are, but they know that you call your wife every day at a certain time, and they can say, "Gotcha!"

The only way to use a burner phone where they don't track you is to use it only once, and then you throw it away. You watch old spy movies; they learned that.

The only secure way to use a burner phone – in a secure way that is slightly safer – is to use two burner phones for both parties (one on each side), and use it only once. Beyond that, it's not very useful.

So the answer is this: Don't use burner phones. Use Signal or Session or use something else. Burner phones are an out of date solution. They are for drug runners.

Lynn: There you go! So, what would you recommend for a computer system? Are we talking Linux?

Braxman: Yes, there is no doubt.

Many of my videos talk about the fact that Apple started putting AI tracking in your content (pre-encryption) to look at your pictures or whatever is on your device. They use the AI to give instructions to spot the content before you encrypt it and send it over the air. That is the new thing they are doing now. They are passing a law in the UK to require that kind of behavior. Their excuse is that this is going to be used for CSAM (Child Sexual Abuse Material) or illegal photos of minors. So they are using that as an excuse.

"We will spot any traffic on any device", and Apple implemented that first.

Lynn: How long ago have they implemented that? Do you know?

Braxman: Apple already has the technology to do it. They claim they haven't started it, but they have the technology to do it now. The UK hasn't passed a law yet, but they are trying to do that. Signal just released a press release saying, "There is no way that we are going to allow that on Signal," even though whatever law is required. They will just leave the country. They can't really enforce it with people using Signal. You can download the Signal app without using any app stores. You can't block signal from anything.

The only device that we know for sure that doesn't have any of that is, of course, Linux. I use Linux myself.

Windows can be set up to remove the spyware; you can probably remove 99% of the spyware. I have a set-up video for it. You can do that, but you can't do it to a Mac OS. If you are going to use a Mac, you are as good as done; they've got you!

Lynn: I have one last quick question, and then I know we have to wrap this up. I think that open source software is really important. I ditched Microsoft Office a couple of years ago for several reasons, aside from having to pay them

to scrape all my data. I went to open source LibreOffice.
I want to get your thoughts on another way to save money and hopefully, prevent even more of your data from being scraped by going with open source versus some of these software programs where they want you on these subscriptions.

Braxman: I use LibreOffice, so that confirms that. I do not use anything in Microsoft Office. I'm using Linux, so that already limits me to using mostly free solutions for things.

When you use Linux, you will tend to be using free software and open source software. It's the 'nature of the beast'.

White: Rob, this has been a great interview with great information. Where can people find out more about you and find out more about your phones and everything you have going on with the mail server and all those things?

Braxman: If you're on YouTube, I'm 'Rob Braxman Tech' on YouTube. I have a big channel there. I'm also easy to find on www.Rumble.com. I'm 'Rob Braxman Tech' there, and I'm also on www.Odyssey.com., on 'Rob Braxman Tech' there. I'm on Twitter with the 'Rob Braxman Tech' name, but YouTube is the one where I have the most subscribers. You can follow me there.

White: Corey, is there anything that you want to say in closing?

Lynn: Rob, what is your website?

Braxman: My website is www.Brax.Me. I made my own social media platform for the privacy interested people. I have close to 100,000 people on there. There is an app for that as well, or you can visit the website. That is where you find the community and the store and my products. You can talk to people in the community there.

Lynn: Thank you so much. I really appreciate this, and I think this will be a big help for people.

White: This has been great. Go to www.Brax.Me. We have come to the end

of another podcast here on *The Solution Series*. We do appreciate you supporting the broadcast. You can find out more about *The Solution Series* by going to www.CoreysDigs.com or *www.Solari.com*.

For *The Solution Series,* this is James White saying goodbye for now.