Episode 871: How to Keep the Spooks from Snooping Through Your Email

Guest: Alain Ghiai

WOODS: Before we get into details about different countries, different privacy regimes and different laws that are in place, particularly in the United States, why should the average person care about any of this? I mean, I think, even though I talk about politically sensitive and unpopular things, if anybody got into my email they wouldn't find anything incriminating. It would be annoying. I wouldn't be happy if someone was snooping around in my email, but it's not like I'm going to jail for it. So just to play devil's advocate, why should that bother me? The prospect that somebody might sift through it, why shouldn't I take the attitude that I have nothing to hide, so who cares?

GHIAI: Right, this is actually a very good question, which most people would tell me. And I would put it to you this way: imagine somebody following you in every aspect of your life, from the time you wake up, even while you sleep, shadowing you all the time. You wouldn't like that too much. And this is a metaphor for what's happening today in the age of the Internet. So no, we don't have incriminating emails, but we do have one of the few things that is left in today's technology world and social media, is really the privacy of ourselves, our individual privacy and what we do want to reveal and what we do not, because so much of our lives are already open to everything. You put something on the Net, on Facebook, you're going to put a photo, even if you delete it, there will be a trace. There's now a marker for life. So privacy is important because it is one of the few things that's left that we still somehow control.

So I'm going to give you a quick example. Let's say you're going to email me about a new Cadillac that you bought. Well, this is a harmless email because you're going to show the Cadillac to everyone and everyone will see you in it. But Cadillac itself will know that either you bought one or you're interested in one — and this is through the Google social engineering. Most people use Gmail or Yahoo, free emails, basically that essentially take our entire data and sell it to companies willing to buy it. And I'm not even going to talk about the government intrusion. Right now it's just light intrusion, which is commercial, and they're going to pump you with stuff about Cadillacs. So that's a classic example.

So as far as I'm concerned, I don't want some robots in the Net knowing what I do, what I buy, what I feel like. That's what privacy is about today.

WOODS: I would think also, I'd bet even the most innocent folks, who think their email accounts are just full of links to cat videos that they're sending to people, may have some embarrassing stuff in it that if somebody got hold of it they could use to blackmail that person or make that person's life very unhappy. So even if you're not trading military secrets with the Russians, you might still have stuff in your email that you wouldn't want generally known.

GHIAI: Absolutely.

WOODS: We see headlines all the time about violations of email privacy. There was just an article in The New York Times at the end of 2016 that told us that Yahoo had engaged in systematic scanning of all Yahoo users' emails looking for something the government was asking it to look for. So they weren't poking around a little bit here and there; they systematically scanned the accounts of every single user of an address that ends in yahoo.com.

GHIAI: This is actually a really good point. So the first harmless way was, I'm thinking of buying a Cadillac. That's okay. Now you're looking at another level of privacy intrusion. And you may have embarrassing cat videos; you may have more than just an embarrassing cat video. And then a level above that is basically government intrusion, which happens all the time. What you read in The New York Times was basically the work of investigative journalism. But this happens every day.

I'd like to talk about the big five. The big five are Google, Microsoft, Amazon, Yahoo used to part of it — and well, now there are probably four of them left. These large companies, which are indirectly funded by the government because — and Apple actually was the fourth one. These companies essentially work for making money for the shareholders, but they do work for the government as well. The Yahoo article just showed one incident, but it happens daily.

You mentioned about scanning emails. So this is a request of the government. That was I think you mentioned in 2016. There is a law that passed, I believe the Cybersecurity Law of 2015. It passed in December very quietly. And essentially it makes it much easier for a government entity in the U.S. to literally just own that entire data and scan it. I read a lot about articles about the government agencies spending hundreds of millions on servers. Basically the budget of the FBI and NSA are pretty much limitless, so it's in the tens of billions of dollars. So they do have the budgets to literally read everything. Now, nobody goes behind and reads it. These are done electronically through robots.

But it starts with a law that passes that says now we're going to get an automatic feed. Let's say you type or you say a word that will trigger an agency, a word that — it could be apple; it could be anything that the government decides. And during that conversation, that word is there. It is automatically flagged and goes to the governing agencies. And that is a big problem, because essentially you have zero privacy at that level. This is part of the U.S. Patriot Act and all of the other laws it passes. So yes, that was a heavy intrusion, but it happens all the time. It used to be that the

government had to ask the telecom companies like AT&T and Verizon and so forth for that data, and now it's automated. This is I think since the Cybersecurity Act of 2015. So what you read in The New York Times was a lucky break because finally sometimes some information leaks out, but this happens daily.

WOODS: Now, I'm reading from a recent filing to a U.S. district court where Google says a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. Google, of course, is a third party. Now, Google's a private company. If it wants to have crazy policies, that's its prerogative. But I bet most people — my point would be: I don't think most people realize that. I think they assume that these are all private communications and they should probably be aware that in the final analysis, they're not.

GHIAI: No, you're right. And two things I would like to point out: this is for the average consumer. A third party in the business world could be a legal entity, a lawyer, and so forth. This law is very — it touches a lot of sectors. it touches you sending a cat video, but it also touches a court case or a huge case between companies, legal cases. If you technically volunteer that information — because you do use Google for free, mind you — they own that information, and then with the help of the law they can essentially tell you, well, you volunteered that information.

I want to talk about the second point. Google is no longer a private company; it is a public company. They have massive government contracts just like Apple and Amazon. So the lines get blurred at this point.

WOODS: And that's fair enough. Now, I'm glad you raise that point, because we might talk about differences around the world in financial privacy in different countries, and we associate Switzerland with greater financial privacy or the Cayman islands or whatever. But when it comes to electronic data transmission and emails, here it seems like things would be somewhat different because even in different countries everybody's still using gmail. And so this presumption that we're not necessarily going to keep your data private would seem to follow you anywhere in the world. Or am I wrong about that?

GHIAI: No, this is right, and you touch on a good point: the data privacy laws. So I'd like to clear up a couple of things. So it is true that Switzerland was a haven for a private bank account and for privacy in the financial sector, and since I think as of 2018, there is a global information exchange agreement, which was pushed, by the way, by the United States. The OECD, the U.S. didn't sign the agreement, but every other country had to. You may have read about Swiss banks hiding U.S. citizens' money and paying billions of dollars. So the Swiss banking secrecy is pretty much gone for foreigners, but the data privacies are very much there, and it's part of our constitution — I say "ours," because I am from Switzerland, so obviously I know quite well the law.

And if you use Gmail, you basically have no protection. Now, in theory, if you use Gmail and you're a Swiss citizen, according to Swiss law you are entitled to your privacy, but Google, Amazon, Yahoo, all the big guys — and Microsoft — they essentially have to obey the U.S. laws as well. So I think it was about three or four years ago, Microsoft finally admitted that even though they have servers in Europe where they keep all the data and they have to obey the European Union privacy laws, they also have to obey the U.S. Patriot Act.

So the only way to protect yourself is essentially using a Swiss-based company, and then the company can be prosecuted if your information, because neither Google nor Yahoo nor Microsoft nor Apple, none of these companies are tied to that Swiss law only; they're also tied to the U.S. laws. And of course they are U.S. companies. So if you use Gmail, you're not protected. If you use a Swiss-based service — let's say there's others as well — you are protected globally because the data that resides in that particular country from a particular company, that's the law that's applied to. So if I tell someone that you have an account with our company, I could go to jail because that is a privacy law that's very strict. In fact, Switzerland has revised it with the European Union not too long ago, and they made it even stricter.

WOODS: All right, now I want to raise the issue of your own company, DigitalSafe, and I want to tell people you guys reached out to me some time ago to see if maybe your product might be a fit for my audience and maybe I could — thought maybe I might run an ad or two. But then when I looked at it in more detail, I thought, no, I've got to do a whole episode on this, because I actually ran it by a previous guest that I had who's an expert on this stuff, and I said, This looks really good to me, but I'm at a second-grade level when it comes to stuff like this. I need you, an expert, to tell me is this product useful and any good. And he came back saying, This thing's unbelievable. I can't believe I didn't know about it. I love this. Yes, it absolutely is useful. It absolutely is a good idea.

So I want to tell people and be as above-board as I can that I have an affiliate relationship with you guys, but at the end, I will give two links. I'll give the naked link if you don't want me to get a commission; you can just use that link. But if you're okay — it doesn't cost you anything extra — with the show getting an affiliate commission to help keep the lights on, I'll give you that link also. But I want you to tell us about DigitalSafe and how this all works. It is super intriguing and I love it.

GHIAI: Thank you. Thank you, Tom, for being a believer in our product and also for valuing our privacy laws. So DigitalSafe simply put is a virtual vault in your pocket. So it's a Swiss-hosted service. We are a Swiss-based company. And DigitalSafe is like a virtual bank vault essentially for all of your electronic data. In the old days you went to your bank and you deposited your papers; your important papers were kept safe. And now everything is electronic. So it's the same concept.

It's a web-based service, accessible from any computer and phone you want, and it can store all your documents, information. It also comes with a password manager, which is very convenient because we all have a lot of passwords to remember and to create.

We definitely don't want to use the same passwords for everything. And it also — one of my favorites — it comes with a Swiss-based secure email.

And I want to talk a little bit about that because it will go back to our Google Mail thing. So when you sign up to DigitalSafe, you have essentially your bank vault in Switzerland, electronically, of course. And whenever you connect with it, you are digitally in Switzerland. This is important, because we strictly obey only the Swiss data privacy laws. We are not bound by any other laws in the world except Switzerland. That means that I would not be able to divulge who owns an account with us. In fact, we can't even see into your data because we have specific technology that doesn't let us see what's in your bank vault, etc.

The email is interesting. So we have a feature called Secure Send, and if you want to talk about the Cadillac that you want to purchase, Tom — I'm not implying anything, but let's say you want to buy a Cadillac and you don't want Google to know about it, but you're sending it to someone who has Gmail who hasn't heard of DigitalSafe. You can send your email through Secure Send. It's basically a way to send a link to the recipient with a password protection. It has a time limit where the email self-destructs and all sorts of fun things, and it's very easy to use.

And the recipient, once they have a password they can essentially read your email. They cannot reply because they would need DigitalSafe, or if they replied they would use their own email. But your content remains private. Essentially, both of you are in Switzerland when he or she reads that email and you send it. That means that even if Google is the provider of the recipient, the email provider, Google will not be able to read the content. This is massive. You can also have time expirations and so forth. It's very easy to use. We have a lot of videos on the website. But the concept is really simple.

There is no longer financial privacy in Switzerland or in the world. This is all changing with the automatic exchange of information, so we figured, you know what? We will make sure that the data privacy still is useful. And in Switzerland, we have a law — well, a couple of laws — that value the privacy of the individual and of corporations — so an entity. So if you are a Swiss-based company, privacy rules. If you're a person, your own privacy is very valuable. That means that nobody can go and really pry into your privacy. Switzerland has the strictest privacy laws in the world for data and personal privacy. So that's it. You use a service; you have it on your phone or your laptop or what have you. And every time you connect, you're basically in Switzerland.

WOODS: So I would have to create a new email address for this?

GHIAI: Yes, so if you're an individual and you buy a regular package — I think it starts at $9 or what have you — it depends on how much storage you want — you will have an email @DigitalSafe.com. But if you're a business, actually — it's a new feature that we have — you can choose to have @DigitalSafe.com or, let's say, @TomWoods.com. So if you're a business owner, you buy a business package — I think they start at $25 a month for five users — then you can configure your domain email so that it is hosted in

Switzerland. You get two things. You get a highly encrypted system to start, so you know it's going to be basically very resistant to hackers, and also you get the Swiss privacy laws. So you can configure TomWoods@mycompany.com. And nobody will know that your company is hosted in Switzerland.

But what's important is, let's say, in the business world especially — you have a lot of subpoenas, you have law suits, you have things like that — we try to tell people it's not about hiding from subpoenas; it's about giving the other person a fair chance for preparing themselves for a legal argument or what have you. So that's important. As a business, you've essentially put all of your valuable data away from prying eyes, and your email of course as well. Some businesses have very sensitive information that they transfer via email. You have technology, pharmaceutical, financial — I mean, I send all my bank statements or tax returns to my CPA through DigitalSafe. There's also a file sharing system in DigitalSafe, so you can either email someone or you can send a file share. The recipient doesn't need to have the account; they just need a password to open the file share. The beauty of it is that everything resides in Switzerland.

We are a private company and we don't owe anything to anyone and we own our entire technology and equipment. So we're not leasing servers on Amazon web services and what have you, because then we would be having to obey with the Patriot Act as well. The minute you use a U.S. company, essentially, you are tainted in a way that you are bound by the U.S. privacy laws, which are very bleak.

WOODS: All right, let me come at you with a worst-case scenario. And sometimes, by the way, worst-case scenarios are not as helpful to clarify thinking as you might think, because, for example, suppose I had a small country that was completely free market. Even the military was free market. And I say, How would you be able to withstand the Nazis? Well, even a regular government in the small country wouldn't be able to withstand the Nazis, so it's not really a fair thing to say. But I do want to consider the possibility that the U.S. government is going after some guy for whatever reason and he happens to have an email address ending in DigitalSafe.com. What is going to happen to you?

GHIAI: This is a question I usually get from businesses and government entities who use our service. It's a really good question. So Switzerland has updated its cybersecurity laws and this is how it goes. Let's say we have a bad guy. The U.S. first would need to go to the Swiss government because we can only obey the Swiss government, because if I denounce anyone I will go to jail, pretty much. So what happens is if you are a danger to Switzerland — and of course Switzerland will obey if there's an international bad guy, obviously — they will obey, and a Swiss federal judge, one of the seven judges, would have to sign off on a subpoena. And that will take a lot, by the way. And then we would be notified. And then at that point, we have ways to somehow block the account and change the email password, etc. That would be an extreme case. So if there is a bad guy blowing up people and Switzerland would be aware of it from the U.S. government, obviously there would be a request. The Swiss federal judge would have to come to us. So that's normally, obviously.

The other thing is — and we have laws in Switzerland that protect us against people like that. We are allowed to divulge, but we cannot go to a U.S. lawyer — let's say somebody — I'll go to a lower case, a financial crime. The Securities and Exchange Commission is suing, let's say, an executive. If the lawyer for the SEC contacts us, we cannot just give that information. As a matter of fact, in Switzerland we have the obligation to tell that particular executive that they are being investigated because it gives a fair chance. It's about preparing-for-your-case type of laws. So we wouldn't do that for a bad guy, obviously, but for a normal case of a legal battle, we would have the duty to tell the executive, You are being investigated.

As a matter of fact, we would only be doing that if a federal judge, again, from Switzerland contacts us. So it's not simple, but it's not a haven for bad guys either, because Switzerland does have laws that basically shut those down. We are allowed to give away information of international criminals. But again, a Swiss judge would have to come to us.

WOODS: All right, let me ask you what may sound like a silly question, but I mean it in all sincerity. Suppose John Podesta had been using DigitalSafe. Would we have had this whole fiasco?

GHIAI: My answer is no. I mean, basically — and I will even go further, if I may. Secretary Clinton, let's say, who was using private email servers. We even had Vice President Pence, I think, who was also using some private servers. So nobody would know about that because by law it is a crime for people like me to divulge who uses our system. I don't want to go to jail, even if it's in Switzerland. So no, nobody would find out anything, because first of all, we use a highly encrypted system, number one. And number two, which to me trumps number one, is we have the strictest privacy laws in the world. So I think I would say no, nobody would know about it. And maybe some journalists would come to us and say, Does Mr. Podesta have an email with you? I would say, We have no idea who Mr. Podesta is.

WOODS: Hmm, very interesting. Is there any way that something like DigitalSafe — and I'm asking this as somebody who doesn't — I know the gist of it but I don't know the details. There are ordinary hackers who figure out how to hack into people's emails. There's no way DigitalSafe can stop something like that. If somebody's got your password, they're going to get in.

GHIAI: Well, it's more complex than that. First of all, I'm going to give a one-minute quick lesson to people out there about encryption. You have essentially two main encryption types. One of them called PGP, pretty good privacy, which is not really that good — it's an old technology — it lets the users themselves own the encryption keys to their email, their safe, or what have you. And whenever a message is sent, that encryption key is sent with it so that the recipient can decrypt the message. In those instances, which is WhatsApp and Telegram, all these applications use that — in those instances, a hacker can come in, intercept the message, and own the encryption key without your knowledge. That's, let's say, 98% of the products out there that use that.

We use a different system. Our philosophy is we will keep the encryption key, because we're probably more responsible than you and we have a few million dollars of machines to keep that. And then all you have to do is put your password in. So no the front end, it's super easy. ON the backend, unbeknownst to the user, there is a lot of things that are happening in decrypting and very long encryption keys and so forth. So we do have a higher encryption. We also have a third party auditor that basically every 90 days tries to hack everything we own, and so far in the last ten years that we've been in business, we have never had a successful breach.

Now, let's assume somebody breaches us. The way we keep information is splintered in millions of bits that even if you're able to hack into our server, you will never get and reconstitute the message itself, so you will never get 100% of the data. So it will be a lot of gibberish. We also have some technology that we are implementing the next few months which gives us biometric login. Those are for enterprise and government. So we always innovate. I never say nobody can breach us, because that would be foolish. I'll have to say that we have a 99.999% success rate. Never 100. You just never want to say 100%.

WOODS: Well, it's all very interesting. And again, I'm sorry I'm kind of a technical dolt when it comes to stuff like this. But in a way, if I were to use DigitalSafe, that would be one of the benefits, that this is how a technical dolt can protect himself. I mean, I've heard all about encryption and I know about all kinds of things that I've heard about, but I wouldn't know where to begin in doing any of it. That's the problem. It's not user friendly — it's not newbie friendly. I'm a complete newbie with stuff like this, and I could just join DigitalSafe and use it. That's why I like it.

Whereas I think there are some other solutions that — My view is if you can't explain it to your grandmother, then you don't really understand it. And if it can't be explained to your grandmother, then it's not really ready for primetime, as we say. So that was why when you guys contacted me, I looked at it, I ran it by my resident expert; we all decided that not only is it great, but I actually get what it is you're doing. I can explain it to people. I can explain it to other people's grandmothers even, as a matter of fact.

So people should definitely check this out. The naked link is DigitalSafe.com. My affiliate link — doesn't cost you anything extra but helps me keep the lights on here — is TomWoods.com/safe.

GHIAI: If I may say something, Tom, to your audience, if they use your link, they get 30 days for free. We do not offer a free trial.

WOODS: Oh, well, then, now you're starting to think out there in cyberspace, aren't you? Now it's becoming a lot more attractive to use TomWoods.com/safe. I must not have been reading the emails carefully enough. I did not realize that — I would have opened with that if I had known my link had that special benefit [laughing]. All right, so TomWoods.com/safe. Of course I will link to all this stuff at TomWoods.com/871, our show notes page for today. But here you go. If you feel like sometimes we get so bogged down in negative stuff, here's something great. Here's something that actually

does something about the things we complain about. And once in a while, it's nice to be refreshed with news like this. So I appreciate your time and efforts on this very much and thanks so much for being here.

GHIAI: My pleasure, Tom. Thank you for having me.