CB: Hey everyone, this is Craig Ballantyne from internetindependence.com. And I'm here today with my friend Simon Black to discuss a topic that you probably won't hear a whole lot of other people talk about, which is online privacy and registering your websites so that you are protected and you're protecting your business. So Simon, welcome to the call.

SB: Thanks.

CB: Simon, why don't you tell us a little about your business, which is sovereignman.com, how that first of all got started, the mission of that business. And then we'll talk a little bit about how you have your website and hosting and all that registered to protect your business.

SB: Sure, yeah. Our site sovereignman.com, it's really about maximizing freedom and opportunities around the world. I'm what you would consider what's called a permanent traveler, and I have really no fixed base whatsoever in any given year. I might visit 30, 40, 50, 60 countries. I just really kind of go from place to place. Right now I'm talking to you in very beautiful Santiago, Chile. It's summertime down here. It's bright and beautiful and a very modern first world extremely civilized place with a first rate internet infrastructure. And I think this is the kind of place that particularly people that run internet businesses could probably base themselves and be extremely happy and productive.

What we talk about on our website all the time are ways that people can protect themselves, protect their assets and maximize all the opportunities around the world. And I'll give you an idea of what I mean. And I know there are people really from all over the world who probably are listening to this, but I'll just pick one country for example and just say the United States.

If you're let's say a US citizen and you live in the United States and you work in the United States, you run your business out of the United States, you have a US corporation or LLC, you bank in the United States, you own your home and your property in the United States, you have US investments, all these types of things, you're obviously very focused on everything in the United States. If something goes wrong in the United States, and it doesn't have to be anything extreme, it can be something as simple as – an example I give a lot is your neighbor's kid falls in your swimming pool – or you get divorced or one of your employees decides to sue you for some kind of wrongful termination, sexual harassment lawsuit, you name it there's a million things that can happen.

And suddenly with all of those assets and interests that you have ranging from your home to your website, your domain, your merchant account, all these things that you have that are very central to your life and your livelihood, all that now is in jeopardy because any judge, any bureaucrat who works for some three-letter agency, whether it's

the FTC or the FCC or the SEC or the FBI or the IRS or a million things can really at any given time with a couple of mouse clicks freeze all of those assets and interests that can shut down your bank account, they can confiscate your domain, all kinds of things that can really throw your life upside down.

In the Western world and the free world as it's so often called, the free world kind of prides itself on this burden of proof where somebody who's charged with a crime is deemed innocent until proven guilty. And that's not actually really true, particularly in administrative matters. In a lot of cases you are presumed to be guilty, and then they take away all of your assets with which you can prove your innocence and then expect you to prove your own innocence, whether it's some kind of tax trouble or something like that or regulatory trouble.

In the US they have this thing called the CAN-SPAM Act. And anybody who might have missed a couple of minor disclosures on an e-mail marketing campaign might be in violation of this, in which case any number of three-letter agencies can go in and literally seize their bank accounts and put a levy on their homes and all kinds of things from just minor transgressions. And it really leaves people defenseless to be able to defend themselves.

So these are the kinds of things that we talk about on our website. We have a daily email and we talk about this in our daily email, ways that you can really mitigate this risk. And it's quite easy really to mitigate the risk by really diversifying your assets and interests across a variety of different jurisdictions.

CB: **The whole reason we got on this kind of conversation, you and I, over email and it's gone into this phone conversation, is because back in I think December a friend of mine had sent me an email about the United States government starting to seize domain names and websites just because they can do it and you can't stop them from taking your domain name if it's registered in the United States.**

So why don't you tell us a little bit about what you've done to protect sovereignman.com. From what I remember you have your domain registered on the moon and your site is hosted on Mars I believe.

SB: Right. It's actually Venus, yeah you're right. To give a little bit of color to what you're talking about, it wasn't too long ago, you're right, the Department of Homeland Security in the United States decided that it would start seizing domains, internet domains, that it deemed – in its sole discretion without any due process – in its sole discretion it would start seizing domains that it felt were violating some kind of law, whether it was file sharing, copyright infringement or just sort of anything that it didn't think was up to snuff. And stuff started happening.

In fact, I've got a picture I can send it to you if you want to put it on your website Craig, of sort of the new landing page – when Homeland Security seizes these domains – there's a new landing page that says "This website is now the property of the Department of

Homeland Security". So needless to say somebody that makes a living online based on a website, it makes it pretty difficult to do business if you don't have a website anymore. And when the Department of Homeland Security is just moving straight to seizing your assets, your electronic assets, without any level of due process whatsoever it's a pretty scary process. And I think anybody that does anything online, particularly web-based businesses, should sit up and take notice of this and do an inventory of their own electronic assets and figure out what's at risk and what they can do about it.

The nice thing is there's plenty of things you can do about it because the internet is really the great equalizer and it puts a lot of countries on an even playing field. I guess I can use ours as an example. Let's look at what most people do. They want to run xyz.com so they go to something like GoDaddy to register xyz.com and they run their business. They have their merchant account in the United States and the merchant account pays their bank account which is in the United States. And their domain is registered to their US business. The intellectual property, whether it's the ownership of the domain or the email marketing list, all these kinds of things are owned by their US company or their US LLC, or maybe even individually. The contact information for their company in many cases is their home address, something like that. It's a lot of really personal exposure to these things.

And you've got to believe that, particular somebody like Bob Parsons over at GoDaddy, the US government's going to come knocking on his door and say, "Turn over xyz.com." GoDaddy's going to do it in a second. I think a lot of these, particularly larger US-based companies. They'll sell anybody out down the river in a second. The same thing goes for email. People are really heavy Gmail users and you just have to – ironically go and Google some of these cases or use any search engine you like. But Google has turned over email accounts, frozen email accounts. There are just tons of these cases.

I remember one case in particular where there was a bank employee, I think this might have been last year or the year before, I don't remember exactly, but there's a bank employee somewhere that sent some kind of financial records to a customer, into a customer's Gmail account, and did it by mistake. And the bank employee noticed his error and started emailing the customer saying, "Hey, I just sent you this by mistake. Please respond back to me and let me know that you will destroy that e-mail," and so on and so forth.

I don't know what, if the guy was on vacation, but he wasn't checking his Gmail account, didn't answer. And by the time I guess he got back from vacation or whatever Google had frozen out his email account and he was restricted access to his own email account and the bank had gone and petitioned some judge to freeze his account and force Google to turn over the emails and all these things.

And anybody who gets sued, which basically I think is anybody who's really achieved any level of success I think at some point in their life ends up getting sued. Emails these days are used as evidence in lawsuits all the time. And during the discovery process it's very common for peoples' emails to either be frozen or have all the contents of their

emails confiscated and turned over. And I know this has happened to a lot of people. It's a pretty scary thing to see that level of invasion of privacy to be sitting in a courtroom and watching some email that you were sending to your buddy joking about going out to the club the other weekend or something like that and being thrown up on an overhead projector in a public courtroom, this sort of thing.

There are a lot of things that really can happen. And I think what we're doing personally, and what we encourage people to do, is to diversify all these various assets and interests overseas. You mentioned we're hosting our account on the moon and all this kind of stuff. It's true.

We spread as many of our electronic assets to as many different jurisdictions as possible. It sounds complicated but it's not. We have our bank account set up in Hong Kong. We have a merchant processor that's based in the United Kingdom that pays a company that's based in Singapore. We have a Columbian registered domain that's registered through a Swiss company, a Swiss registrar. And we hold various intellectual properties on different servers around the world. We have a Norwegian based email server. We have a Canadian Web server.

And so what you see is we really spread and diversify all those things all over the world so that there's not really one government, one jurisdiction that has any level of control over us. If anybody decides for whatever reason that they want to come after us or they just decide they don't like our content they can start seizing assets and domains and things like that. It makes it really, really hard to do.

It's almost like having The Club on your car, you know what I mean. It's like a thief walks by and sees it and just decides, "Okay, well I'm just going to go on to the next car that's a little bit easier target." When you kind of diversify this stuff around you've got to trust in the Cook Islands that owns a Singapore company, the banks' in Hong Kong and processes accounts in Europe that has based a domain in Columbia and serves in Canada and emails in Norway. It's too difficult of a target for anybody and they just kind of shrug their shoulders and move onto somebody else, one of these guys that runs his website from his buddy down the street and uses his home address as the contact information on AWeber and all this sort of thing.

So there are a lot of options out there, but the point is I think people need to take an active responsibility in diversifying their electronic assets in order to reduce and mitigate this risk.

CB: Would you be able to maybe point us to first of all what's kind of the most important thing to diversify immediately, because again anytime people get new information it's a state of overwhelm and it's like, "Oh, there's seven different things he listed there. I live in America. I don't know how to find these reputable companies." So first of all, maybe what are the one, two or three most important things to do right away? And then second of all, some tips on finding reputable companies in different jurisdictions.

SB: Yeah, that's a good question and you're right. And I think for people that don't really have a whole lot of experience it sounds complicated at first. I'm here to tell you it's really not that complicated when you think about it. You start a business you need to register a domain. So what do people do? They go to something like GoDaddy. Well, instead of going to GoDaddy you go to another service that's based overseas, one in Switzerland or Panama or a variety of different places.

You need to establish a bank account. You need to establish a corporation or some kind of LLC. So instead of doing it in your home country you ask for Canada or wherever you happen to live, you do it in another location. You do it in Singapore. You do it in Hong Kong. You have to establish a bank account. Instead of establishing a bank account in your home country you establish a bank account somewhere else. You establish the merchant account somewhere else. So it takes a little bit of extra legwork, but it's not really complicated.

I'd say the most important thing, to your specific question, the most important things that people ought to watch out for are specific to their individual needs depending on the nature of their business. I would suggest that people kind of start by looking at what are the most important elements of their business. If you run for example a free daily blog that's entirely Web-based then probably your most important asset would be the website, would be the domain. And so I would think in that case the best thing that you could do is just switch registrars basically, from if you have a registrar in your home country move to another registrar overseas where another registrar would be able to control that.

And then consider doing the same thing with your Web servers. So if your Web servers are based in your home country, look for Web servers in another country. If you're in the United States look for Web servers in Canada. If you're in Canada look for Web servers in the UK. There are really a lot of options in the world. And I think people are accustomed to sort of looking in their backyard because it's easy, but there are really a lot of options out there. There's companies that specialize in providing, whether it's Web servers, email servers, the whole range of products all over the world: South Africa, Argentina, Brazil, Panama, Mexico, all over Scandinavia, Japan. You name it and you can get it anywhere in the world really. It just takes a little bit of extra research.

I think where everybody would want to get to eventually, particularly if you're doing a lot of electronic commerce, is probably the point where your banking and your financial transactions are offshore as well. You can set up offshore bank accounts and you can set up offshore merchant processing. I know this is kind of a dirty word for a lot of people. They think that if you do something offshore that it's inherently illegal or there's something shady about it. And the fact of the matter is it's not. There's absolutely nothing wrong with it.

There are some additional disclosures that you might have to make, depending on your nationality. If you're a US citizen, for example, and you have offshore bank accounts you need to file a form to the Treasury Department every year by June 30th. It's TDF90-22.1. And there are a few disclosures. You check a box on Schedule B of your 1040

and some other things, but it's really peanuts in terms of the administrative hassle. It's really no hassle at all. And the peace of mind that you get knowing that you've substantially reduced the risk in your business is worth far more than any minor hassle of having to fill out a couple forms every year.

CB: Just to be very clear on everything that you're saying here, it's all legal and it all comes with a different level of disclosure that you have to make. But certainly everything that we're recommending here, it's within the law.

SB: Absolutely.

CB: Not to get into too much minutia on the recommendations for different countries, but where do you have to make a decision on, for example, if I'm in Canada and I have a Web hosting in the United States, those two countries are so closely linked in the legal system that for all intents and purposes something like that it's almost like being in the same country. Is that something that's right to say, or do I have to get more exotic with –

SB: The rule of thumb is you never want to – there's no reason to ever go overboard. And you don't ever want to do anything that's going to be detrimental to your business for the sake of decreasing the risk to your business. It just doesn't make any sense. It's chopping off your left hand to save your right. It just doesn't make any sense. So that being said, it might be ideal if you can move – and again, there are a lot of countries that you could host, there are really excellent hosting services in places.

And like I said, you want to pick the places that are renowned for high quality service, very strong high-speed internet infrastructure and in places where English proficiency – sort of match your primary language – English proficiency is fantastic. So I'm a big fan of if you're looking to come outside North America, which if you're North American-based like me, it's a reasonable idea to look outside of North America. You're right to a degree. There's a lot of – there's some close legal ties between Canada and the United States. So if you're looking to get outside of North America you could look in Scandinavia, Norway, the Baltic countries, Sweden and Finland even. There are really some great services out there.

People think because it's Scandinavia it's not English speaking. But I would wager that probably the average Scandinavian speaks better English than the average American, mostly because they've been studying it since they were children. They have world class internet architecture, really just fantastic. Very, very fast. I think that actually Scandinavia internet architecture is better and more efficient than it is in North America to be honest with you. There are some services in Japan as well. And I think Japan really has some of the fastest internet infrastructure in the world.

So to your point, again I think bottom line is you don't ever want to do anything that's detrimental to your business. And if you find that moving overseas to a place like Norway or something like that would be difficult for you then don't do it. And you could

move to a place like Canada or something like that it would be fine. There's no reason to go overboard and I think kind of use common sense as your basic approach when you keep these risks in mind.

CB: Awesome, appreciate that. Now we've covered pretty much everything about setting up the website stuff. So let's talk a little bit about email privacy and even surfing the Web privacy. I know you've mentioned to me in the newsletter a service called Cryptohippie, I think that encrypts your Web browsing, and then you talked about having an email where the company's email servers are in another country. And that kind of overlaps with our last question, but let's say that somebody doesn't want Google and the American government to know what websites they visited or what they're emailing out. What would they do then?

SB: Well, browsing the internet is something – it's insane how much of your personal Web activity is archived. Everybody should realize that all these things they do online, particularly if they have a Gmail account and they use Google a lot. Google's going to follow them throughout their entire Web experience. They log into their Gmail account, Google knows it's them. And I don't mean to pick on Google. I mean Google's a great company and they provide valuable services that people enjoy. And in most cases it's free for people. And I don't mean to disparage Google or anything about the company's reputation. I'm just surprised at how much people kind of give up such a huge part of their life to one company.

Google has the Surge and it has the email. And I remember for me the one that really floored me was Google Voice, when they launched Google Voice, because now you have this one company. I'm in Google Maps in the geo location and everything like that. So you've got this one company that knows where you are and knows who you're talking to. All the emails it has archived every email that you've ever sent, because they give you however many gigabytes for free so you never have to delete anything. And now you're making your phone calls. It has a record of all of your phone calls, all of your voicemails, all of your entire contact list for both phone and email.

So there's this one company now that just has so much oversight of your personal life. And I couldn't say anything – I'm not saying that Google has any bad intentions. What I am saying is that they are, particularly if you're a US citizen, they are in the same jurisdiction as you. And so if something should go wrong again, suddenly your entire life can be subpoenaed. Or a few clicks of the mouse or a keyboard and some bureaucrat freezes all these things or gets a copy of all of these things and suddenly again, all of these things, your location, your voicemails, your emails, your contact list. All of your Web history, all of your Web history, has now been subpoenaed, it is a matter of record for whatever, there's a lawsuit against you.

I mean there are these things that they can use to paint a picture against you, to incriminate you or fine you or all kinds of things. And it's just, to me there are some very basic things that people can do to protect themselves, protect their privacy so that these things really aren't under the complete control of one company.

You mentioned Cryptohippie, that's one way that we've recommended in the past to surf the Web much more privately. Cryptohippie is a service, it's a subscription service. There are a lot of these kinds of proxy servers out there. A lot of them, they do a basic job. They're kind of low tech, rinky-dink. But Cryptohippie is a very professional service. It's a subscription model. The architecture is structured in a way that it bounces all over the transmissions around through various servers around the world and it encrypts everything.

So it makes it pretty tough to – nothing's really foolproof or impossible to impenetrate online as you probably know – but it gives you a much, much, much greater level of privacy as you do things. We've actually negotiated with the owner and we're able to give away a very substantial discount to the service through our website, and I think it's a pretty valuable thing, people if they're interested in internet privacy.

The other thing that you mentioned was email – and again, going back to the Google example or any of the other major services, whether people have MSN or Yahoo accounts or something like that – again these are all places that are under the jurisdictional authority of most of the time peoples' home government. And there are a lot of different options out there for people. If you live in North America it might be a good idea to just use another email service somewhere. There's a ton of them, again, all across the world: Scandinavia, Singapore, the Philippines.

And in a lot of cases you might not even really have to change your email address. Like for you Craig, for example, you could change your domain and just change the MX servers to whatever you use. Let's say you use Gmail right now, Google does the Google Apps where you can host your own personal domains email through their Gmail. You can do that. Really all you have to do is just switch the MX servers to another service, something like Runbox or FastMail or any number of other ones that are not based in North America, and suddenly you've got a much greater protection of your email. Suddenly some bureaucrat or court or something like that in your home country isn't able to confiscate your email or shut you down, lock you out of your own accounts and these types of things.

And I think it's a very, very easy thing to do. You can keep your own email address. In particular, if you use a desktop email application like Outlook or Thunderbird or something like that you won't notice a difference at all. The only difference is that the server where your emails are sitting is not in your home country, so it's not necessarily able to be as quickly subpoenaed or confiscated or frozen or something like that at the behest of your own government.

CB: Just a couple of follow-up questions that came to mind there. How long does the company keep the records of your voicemails and your browsing history and your emails and stuff like that? Is that part of your now permanent file?

SB: Yeah, I certainly think so. That's the thing about the internet. Once it's out there it's out there and it's out there forever. And I think the same thing with emails, and now with

Google doing voicemails and things like that. It's all there. I wouldn't imagine that they would purge this stuff from time to time when the cost of storage continues to decline. It costs nothing for them to move a couple extra terabytes, it costs absolutely nothing. I mean it's just peanuts. And for a company that makes billions upon billions upon billions of dollars, spending a couple of bucks on some new terabyte servers is not really a big deal.

CB: I read a book on the weekend called "How to Vanish". And they recommended a search engine called Startpage, which they claim is the world's most private search engine. Now if somebody doesn't want to go so far as to – somebody who's on a budget and can't afford to pay Cryptohippie, is that something that's at least better than using Google and Yahoo?

SB: Yeah. There's a lot of private search engines out there whereby you can – they basically run your search through a proxy server to get to Google, so you basically get the exact same search results as you would if you were searching Google, but without all the follow on tracking and things like that that Google does. So yeah, that's also I think a pretty good option.

CB: Great. And now let's maybe just talk a little bit about phone privacy. I called you this morning through Skype that went through a cell phone. Obviously to me if you're using something like that it's maybe one of the better things to do. Is there anything else that you would recommend? Obviously Google Voice doesn't sound something that's recommended. Are there other things that you want to touch on there?

SB: Yeah. Phone privacy is something that's a little difficult. There's really no form of electronic communication that's completely private. And it depends on what you consider private and privacy. If you're looking for a truly secure form of communication where the only person that's able to receive the transmission is the person that you intend, so nobody's able to listen in and nobody's able to confiscate it and all that sort of stuff, it takes extra measures. There's absolutely nothing in electronic communication that's totally foolproof. Any encrypted code can be broken if given enough time and resources.

Another level of privacy, a lower level of privacy again is one in which your records for example wouldn't be able to be confiscated, stored, subpoenaed, that sort of thing. And that kind of thing, it's a bit more difficult for people that are living let's say in the United States or Canada. Everybody uses their mobile phones. I know there are some people who are advocates of low, low privacy. What they do is they get anonymous prepaid cards. So they go to – in fact, the person who told me about this was J.J. Luna. J.J. Luna is a very well known privacy expert.

CB: Isn't that an oxymoron, a well known privacy expert?

SB: It is, as a matter of fact. Except for the fact that I guess he's able to be well known as a privacy expert because even though people know his name you don't necessarily know that that's his real name and nobody would ever really be able to find him. I'd be willing to suspect that we could put a million dollar bounty on anybody to try and find this guy and nobody would really be able to find him. Nobody knows where to reach him because he follows a lot of these measures. He uses prepaid phone cards and he's got separate addresses for things and he registers his assets, whether it's a website domain or a vehicle that he buys or something like that, through private companies so that nobody necessarily knows who owns it and that sort of thing. So he doesn't leave the trail like most people end up leaving, a trail, a chain, of ownership and location about themselves.

So Luna wrote a couple of really interesting books about privacy. I had a conversation with him not too long ago and an interview we published in our premium service. And he gave a lot of tips about it. And one of the things that he was talking about with phone privacy was using these prepaid cards. I think he mentioned that he uses one from Verizon. And it was an anonymous thing. He gave them a couple of bucks for the SIM chip and he pays cash to recharge it and that's it. Nobody can necessarily know that it's him or that it's tied to him and that's it.

But I think for people that are, particularly Web entrepreneurs, internet entrepreneurs, the phone issue isn't really necessarily one that's a major risk. I think it's a much lower risk than a lot of these other things that we talked about, like the domain and email and merchant accounts and things like that. That's what I'd probably be more inclined to focus on with people.

CB: That's great, I appreciate that. And it was in that interview with J.J. Luna on your website, on your service there, where he mentioned that one thing is that you should never tell people your home address just for regular privacy. And I know that some of our listeners are still using their home address as their AWeber contact address. And that's showing up in emails that's going out to 5, 10, 20, 50,000 people. So guys, please start by making that change and then work your way through the rest of this stuff.

Is there anything else you want to add, Simon, before we leave this call? I know we'll get plenty of questions and hopefully we'll be able to do maybe a follow-up call in the future. But you've answered all my questions for today anyways.

SB: Yeah. The biggest thing is people should understand that it's not complicated. They should understand what the risks are. And I think anybody that does anything online should really understand that there is a risk. In fact, there's a big risk. And if all of your eggs are in one basket it could be very dangerous to your business. And that's the first thing I think to understand.

The second thing is that the solutions are not really that complicated. It just takes the will to act and to actually do something about it. And once you decide that you want to

do something about it there's really a lot of options out there. And the thing with anything online, it makes it really easy to make these kinds of changes. You can switch servers with a couple of clicks. You can switch your email servers with a couple of clicks and all this stuff will be out there propagating to new servers in no time. And it's a really easy fix. And it just really takes the will for everybody to decide individually, "Okay, I've got to do something about this," and decide to make the changes. That's it.

CB: That's awesome, I appreciate that. All right, for everyone listening to this call who found this interesting I highly recommend that you get the Sovereign Man daily email at sovereignman.com. Plenty of information, not just on kind of this real serious stuff that we talked about, but also amazing opportunities that there are around the world. The world doesn't just revolve around America anymore. And so there's plenty of opportunity for people to live and work all around the world and have great success. And so there's plenty of great information at Sovereign Man. So again Simon, thank you very much for sharing your information.

SB: Absolutely. It was a pleasure. And if we need to do a follow-up or something, if there's a lot of questions I'd be more than happy.

CB: Awesome. So again, this is Craig Ballantyne from internetindependence.com thanking you for being on this call. And if you have any questions, please just send them in and we'll get Simon on another call in the future. Bye-bye everyone.

One Last Thing Disclaimer: