**RedZone Podcast Episode #51: How to Use Information in a World of Zero Privacy – Lessons from a Practitioner – with Frank Ahearn**

\*\*\*

Bill: …The things that we did as kids that you did, I did, that we all did in college,
high school whatever it may be. That went behind closed doors and it wasn't public,
now it's public.

Frank: It's the first time in society where children can see the sins of their parents…

Bill: The skip tracing can be done in both legal and illegal context correct? It can be ...

Frank:
There's no fun doing it legally. It's just easy to locate someone illegally. If I'm looking ... Not that I do this today. If I was hired to locate someone and I was going to break the law, basically I would just pretext one of the 5-6 major mobile phone carriers out there because almost everybody has a mobile phone at this point. If they have a phone account I'm going to find them in 15 minutes.

\*\*\*

Frank: Listen if somebody steals your checkbook and they write a check that's considered identity theft. The real question is what is identity theft? Is that really identity theft? No, it's somebody who stole your check. We all perceive identity theft is somebody assumes your identity to that extreme. The statistics bloat it like it's this huge epidemic. Look at what the things they consider identity theft happen to be. They're not really identity theft.

Bill:

[00:01:00] It's interesting. When I was looking ... First of all it's really fascinating to have you on the phone because from the guests that have ... Generally they're business leaders. Business and business IT leaders that are listening to this podcast, but all of us have a personal life as well. We've never had someone with your perspective. I've never had someone on the show. What's interesting is looking at your books you've written over the past 4 or 5 years. Just even the titles of them make me ... Let's go through a couple of the titles. The Digital Hit Man, His Weapons for Combating Digital World. That was your book in 2012. Then you have one, How to Disappear? Erase Your Digital Footprint, Leave False Trails and Vanish. I read that one. I read that one and Big Brother, How to Disappear Avoid Surveillance, Prevent Unwanted Intrusion and Create Privacy in an Era of Global Spying. Then the Little Black Book of Skip Tracing. Creating ...

Frank: That book is doing ... It's shocking it's doing so well. I don't know why.

Bill:
[00:02:00] It's fascinating that book I read. First of all actually I can go all over the map. Let's start off with before we go into the details of these books. Tell me and listeners your story. What's the genesis of all of this? How did it begin?

Frank: I used to do undercover work originally in retail stores like Bergdorf Goodman's A&S, and the various warehouses in New York. I started working in the office running other under-covers. There's a guy in there Scott who was doing skip tracing. I just found it so fascinating locating people. He picked up the phone and he located people. I pretty much wanted that job because to me it was just amazing. Eventually I convinced my boss to give me the job. You have to understand back then in the 80's the early 80's there were very few databases. There was motor vehicle. There was criminal. There was credit. Things like that. You really had to know someone who knew someone who could get you that information. Back in those days there was a lot of brokering of information.

[00:03:00] If you wanted a Texas driver's license you needed to know a cop or a PI in Texas who could get it for you. There was this underground world of information. I got fired from the job and I started working for myself. The problem with using sources from motor vehicles and criminal records and credit records is they dry up. Sometimes they lie about the information. That's when I decided to start social engineering and pretexting phone companies, banks, the police department, Interpol to start extracting information and selling it. That's really the genesis of what I did. I realized I was really good at picking up the phone and lying. Combining that with being able to find that using information, phone records, credit card records, utility records. Then connecting it to locating people, it just turned into this massive business.

[00:04:00] That's where that came about. Going back to I think somewhere around 2000-2001 maybe a little bit before that. The late 90's they had the telephone hearings because they found out about pretext where somebody told General Westmoreland's phone records when he was running for president or something like that. Created this whole massive shut down of the industry. I was still doing the work. What happened was Wolf Blitzer did this report about phone records and it just blew the whole industry out wide. I just saw the writing on the wall. They passed it's either the Gramm-Blily-Leach or the Gramm-Leach-Bliley Act when they made it seriously against the law to pull phone records or pretexts of phone company, pretexts of a bank. I saw the writing on the wall, which brought me into the privacy world. That's the long bloated way around how I became who I am today.

[00:05:00]
Bill:
Let's define the term because I'm in the security business and everybody listening knows the power of social engineering and how employees and workers are the most vulnerable access points into corporate networks. Can you define, what is skip tracing and pretexting? Just so people understand those what those terms.

Frank: Skip tracing is locating people. Pretext is social engineering it just depends on how old you are. That's the reality. It's the exact same back in the day when I was doing it we were pretexting, we were gagging. Then all of a sudden the computer world comes around and they give it a nice name like social engineering. It's really the same thing.

Bill: Got it. Got it. The skip tracing can be done in both legal and illegal context correct? It can be ...

[00:06:00]
Frank:
There's no fun doing it legally. It's just easy to locate someone illegally. If I'm looking ... Not that I do this today. If I was hired to locate someone and I was going to break the law, basically I would just pretext one of the 5-6 major mobile phone carriers out there because almost everybody has a mobile phone at this point. If they have a phone account I'm going to find them in 15 minutes.

Bill: From some of the stories what I find interesting is your ... Maybe you could share one of the stories on how it works? How easy, I was stunned at how easy it was to call in and get records.

Frank:
[00:07:00] Pretext is like dating. Every no leads to a yes. I've always said that in life. You have to understand it's not brain surgery it's a question of how you go about the call. Let's say I need to identify a mobile number. I could basically call into Verizon be, "Hi how are you doing this is Michael Christopher Verizon Activations. We're down over here. I just want to see if you can bring up an account for services." The thing is if it's a young dude I'm like, "Yo dude what's happening? Mike Christopher Verizon Activations. How's your day going? Friday I'm going to the beach. I'm going to have a great time and drink some beer." If it's an older woman I start schmoozing her with, "My daughter's getting married on Saturday we're all very excited."

[00:08:00] You just take somebody away from their job. Customer service sucks. They deal with people's problems all day long. They do this rote thing that has these steps. You can go from point A to point B to point C to point D. Plus the other problem is they're taught to sell, to sell and resolve. They're not taught to protect. I get the right person on the phone. "We're down over here. I just want to see if I can bring up a number to service." "Who are you? Where are you calling from?" "I'm calling from Valhalla, New York." "Oh great you have a call back number?" "No, I'm down so we can't get incoming calls can you bring up the number?" Or I reverse it if I can't get it from Verizon I'll call one of their stores. "Hi, this is Pat Brown with Verizon. I just want to see if you can bring up a number and see if it's activated in your store?" I got some doofus in the store going and boom, "Yeah it's Mike Kelly 10 Main Street Hamburg, New Jersey." That's how it'll work.

Bill: It's stunning. The reason I loved reading those stories right now we're targeted attacks through LinkedIn in and other tools for top executives in companies. This would be a layup for someone in the business that really knew what they were doing. Would you agree?

Frank:

[00:09:00] Yeah absolutely. Do you know what's interesting. People view privacy as strictly a technical issue. They view it as something that's online. They forget about human and physical space. Just take Mossack Fonseca for a second in the Panama Papers company. We don't know if it was a corporate whistle blower or if it was a hacker. It really doesn't matter. It was a human being. To a degree companies do not protect themselves against the human being per se. They just protect themselves against the technology. They're unaware of how information is being extracted in other ways.

Bill: You think right now are there services, underground services that would be able to ... That someone could hire to basically target certain firms and go through these pretexting exercises to extract data for ...

Frank:
[00:10:00] I do that with some of my clients, my European clients. Where basically they'll say hopw would you go about extracting information from our company. Just to give you a very simple example. The difference is you've got to remember if you go in through a hack or something like that. There's always that trace. It's just a question of who's better at tracing you or the other person hiding their digital footprints. If I go in and I pretext someone. You don't see a disturbance to a degree. You'll see somebody may have viewed the information or accessed the information.

It's been accessed verbally. There's no printing or anything of that nature. My clients will say, "How do you get that information?" I can show up at a parking lot of a company and look for the crappiest car in the parking lot. Go and befriend that person. Find out how miserable their life is. Then offer them X amount of 1,000's of dollars for information. Companies sometimes forget this other side. Pretext, social engineering is also a physical thing to a degree. It's figuring out how you can manipulate someone or something to get that information.

[00:11:00]
Bill:
I think that this is huge this type of information that you shared in your books. I think for people in the profession it's a ... I think sometimes it's better to reverse engineer what boots on the ground have done or can do so that you're more aware when you're trying to buy some fancy tool to protect your information. When that might be completely red herring as far as what you really need to be doing is educating employees about potentially being vulnerable.

Frank:
[00:12:00] Exactly. Listen anytime you have a company where customer service is the forefront. That's your biggest vulnerability because you have 500 people who have access to your information. All I need is one. Sometimes companies just ... You know what it is? This sounds really terrible. I just don't think a lot of companies care or see that as a threat or they don't recognize that. They're just concerned that they're going to be hacked because they see privacy as a digital issue not a human problem.

Bill: I think you’re under a huge huge point, mega point. The human vulnerability is actually the biggest vulnerability. It's funny because in a company Frank most of the IT professionals to begin with. Then of that you can have someone who has a clue about security or at least thinks they do. If you're a company with 500-600 or 6,000 employees, if you have 6,000 well educated employees versus a team of 10 IT professionals where would you make your investment? It's obvious I'm just not sure it's making it all the way to the top to make those decisions.

Frank:

[00:13:00] I'll give you an example, one of my clients they wanted to see how predation was on something. This is nothing against outsourcing. Their customer service is being outsourced at a certain time of day. Basically I called in I said, "Hi, how are you doing? This is Mr. So and So and calling from such and such company. We're just doing an integrity testing on our outsourcing. Just want to take a few minutes and see how quickly you bring up the information and access a client’s account." I just went boom, boom, boom, boom, boom. I pretty much got everything I needed. I said, "Listen you did a great job this is wonderful. We're going to be testing other employees there probably about 30 or 40 of them. Please just keep this call private, you didn't speak to me. Don't share this information with anyone." Of course I know the minute I hang up he's telling all his friends sitting next to him that somebody is going to be calling in from the company checking out how good they are at their job. It was just a simple phone call.

Bill:

[00:14:00] I love that. That was a wonderful story I'm so glad you brought that up. When companies are outsourcing their customer service. You say customer service is the biggest vulnerability. You basically just demonstrated how you can exploit really a human weakness to obtain information.

Frank: Exactly. You have to remember also a lot of times customer service will not challenge the other person on the phone, especially if they come off with a sense of authority. I'll be like, "Give me your supervisor, put your supervisor on the phone." Nobody wants to do that because they don't want to get in trouble. They're not used to these things. They're not used to facing or dealing with such issues.

Bill: Let's define about what is the difference between a private investigator, a bounty hunter, a repo service an attorney and a skip tracer? In the continuum from 0 to 10 of the most effective. I should probably put digital thieves in there as well. How would you at least classify skip tracing, PI's, bounty hunters, ropos and lawyers as far as their need to access information. Who do they go to?

Frank:
[00:16:00]
Most of them would go to a skip tracer or information broker. Today they're more underground. A skip tracer basically specializes in locating people or locating information. Private investigators, there are a lot of great private investigators out there. There's what I call the database hound who just sits there and prints out databases and reviews information and tries to crack cases. Then there's the ones who get their hands dirty get in the streets and do what they've got to do. A bounty hunter is just somebody who locates somebody who skipped on their bond. The reality is most people who skipped their bond or escaped from somewhere. They just usually go back to the old neighborhood they're pretty easy to find. Then the repo guy, you have to know the repo guy is given an address to go pick up the car most of the time. That information is uy given to them by the skip tracing department. Some repo guys will pound the pavement themselves and try to locate the cars. The lawyers are just crud, sorry. I'm just kidding.

Bill: No. No. That's fine. I certainly want to get to the heart of the matter here. What about services like Spokeo. Services that have been put in front of the Supreme Court for data brokers. Do you and others in the industry, would you access information from Spokeo or ...

Frank:
[00:17:00] That's just regurgitated crap in plain English because you have to understand that information again if I'm hunting you. Let me just clarify something. When you're hunting someone information like Spokeo, Zabasearch the data base stuff. It's just information. A lot of it is archaic, it's garbage, it's incorrect. The only time information becomes dangerous is when somebody is capable of connecting that information to you in a physical space. All of these database services online. It's just information. You need the guy be it the private investigator or the skip tracer to figure out if you're really there. You could use it as background information. The truth of the matter is if I have your name and your social security number all I need to do is start banging out utility companies in the United States. If I know you lived in New York I'm just banging out Con-Edison, Wilco even though they're not around anymore.

[00:18:00] If you're in New Jersey JCP&L. California, Pacific Gas and Electric. "Hi how are you doing? This is so and so this is my social security number I owe you guys some money can you check for me?" Everybody wants their money. They would be, "Hold on so and so let me bring up your account. You have a showing on this account." "What do I owe you guys?" "52.90." "Hey you guys sending that to my home or the PO box?" "I'm sending it to the home." "Great listen do you have my street name spelled correctly?" Boom, "Thanks a lot." "Do you have the ZIP code down right? Great. Wonderful. Have a good day." Skip tracing on pretext is just chipping away at the stone. It doesn't matter about the information that's online because it's just information. It's like brain surgery for dummies just because it's there doesn't mean you're going to crack open a skull and operate on it.

Bill: Sure. Sure. Gosh. Really interesting. Obviously that book is going through the roof for you which is great. I do highly recommend it. I read it. I really enjoyed it. I highly recommend listeners buy that book. Let's talk about ... Let's move to another topic that is so damn interesting to me. The book you wrote Big Brother, How to Disappear Avoid Surveillance Prevent Unwanted Intrusion and Create Privacy in an Era of Global Spying.

Frank: That's a mouthful.

Bill:
[00:19:00] Yeah. That's a big title. I'm reading the whole title because I want ... I think by sometimes understanding. I sometimes ask people the question do you believe, I think I know the answer to this one. Do you believe there is such a thing as being able to be private anymore?

Frank: No. Privacy is an expectation and a hope and a dream. We never really had privacy. It's just something we thought we should have just because there's this idea of privacy. It's obvious the government doesn't respect it. Business don't respect it, business lie. Take Snapchat for example, "Oh don't worry we'll delete your picture after 6 seconds or whatever it is." Did they? No. The NSA pulling everything and anything they wanted. You have to remember from my perspective anytime you're using something they consider a third party meaning you pick up your mobile phone and you call your wife or your kid.

[00:20:00] You have to recognize that you don't own anything in between that call between you and your kid somebody else does. You can't expect ... You can hope for privacy. You should hope your information is protected, but is it? Only a fool would believe that at this point in society. These are the same people who are posting pictures of their 2 year old kids on Facebook who are Tweeting. Twitter makes sense if you're in business or you're a rock band coming to town. Why somebody is Tweeting about their hamburger or have 400 friends on Facebook or Instagram is to me it's crazy. You can't expect privacy on one end but give it away on another end.

Bill:

[00:21:00] What I like about the book is that I originally picked up the title and I thought Bog Brother, he's referring to the government. You make it very clear that you call it the evil twins, business and government. I love that what do you think ... Let me just ask you this. Why are you picking on bot business and government?

Frank:
[00:22:00] Because I think they're no different. They're both businesses and we're ... I'm not a conspiracy theorist. To a degree we're just like pawns in this game. We see corporate crime all the time. Those with the money get off. Those in the government get off when they commit crime. I just feel like that they're the same entity and they work off of each other. If you're going to think about privacy you need to think about privacy from a government perspective and a business perspectives. I was reading something on Facebook the other day. I don't even know how many users they have, but how much information they garner per minute, per day from their users. It's mind boggling. You're giving it away. Online, when you do things online whether it be a blog, whether it be this or whether that. You're giving your information away so some third party company can make money off of you. To me it just doesn't make sense.

Bill: This problem is very big and it's complex. I know sometimes you hear people say if you have nothing to hide, why worry? What is your response to that? I imagine ... I'm going to let you answer that. I'm really curious I'm sure you get that question at times.

Frank:
[00:23:00] Because innocent people are found guilty all the time. Just because you have nothing to worry doesn't mean you shouldn't worry. Mistakes happen. The truth of the matter is I think what people should think about is ... For example I just use a regular cell phone. I use my cell phone with the understanding that somebody is listening. I think it's your perspective you need to change. When you send that email I don't care about encrypted email what they say that it's encrypted up to whatever, whatever, whatever. Some 14 year old kid in his basement is just yet to figure out how to crack it or maybe he has already. I just think that you have to exist as if somebody is listening to you all the time. You also just because you didn't do anything wrong doesn't mean you can't be accused of it.

Bill: Right. I think what you're saying is the perspective that's most important. Don't have your head in the sand. Just know that that channel is being recorded in some way shape or form.

Frank:
[00:24:00] It goes back to ... I remember when I was a kid my mother would say to me, "Listen Frankie, don't write any notes to any girls unless you're prepared to face what you wrote. You know something that rings true today. Your understanding your actions should always be if I do this somebody is going to find out about it. I have to accept the responsibility. Just because I'm innocent doesn't mean something can be misconstrued.

Bill: Interesting. Let's take porn surfing for example. If a executive in an organization surfs porn on a home device. Obviously a business device or at work would fall under the business rules of appropriate and ... What about from how you're living as a human being if you surf porn. How could that be misconstrued? I'm just interested in hearing your perspective.

Frank:
[00:25:00] Because I think it's a question of one person might recognize that looking at sheeps in pajamas being very disgusting and horrible. Where other people might think that's pretty cool. It's a question of I just think if you do something in life whether it be pornography or write poetry to your girlfriend or boyfriend you just have to stand by and say, "Yeah that's what I do. Such is life."

Bill: Right. Okay.

Frank: Just have some convictions, but if you're going to do something that may embarrass you in life then you really need to think about how you're doing it.

Host: Got you. Got you. That makes sense. I think one of the pieces here in this book about Big Brother you mentioned and the reason I ask that question is because how aware do we need to be of our actions in the digital world. Casually can someone reverse engineer your existence and your habits?

Frank:
[00:26:00] Absolutely. Listen I think the reality is, I always go by the philosophy is if you press enter, send or download that's it. There's no turning back. The bottom line so you have to realize that whatever it is you're doing can come back and haunt you. Whether it be something you perceive is innocent but somebody else might perceive as disgusting or a piece of information that can make your life miserable or communicating with the wrong person. I think it's just a question that comes to you. Listen we all make mistakes in life. The problem with the internet is it doesn't forgive because once it's out there it's just out there. Now you have to face the music. We see it all the time. We'll see a person's name or something that they've done just used as a headline to bring somebody over to another web page. Frank Ahern sleeps with chickens. When the reality is Frank Ahern wrote a book about Sleeping Chickens, that's one of the problems in my perspective.

[00:27:00]
Bill:
I just ran into a friend of mine's son is in college who was walking home from a party at 2:00 in the morning. It was a 2 mile walk. He got pulled over on his walk by the police on campus and was arrested for public intoxication. This friend of mine’s kid is in college doing well. Now his records are online. His pictures are online.

Frank: That's horrible.

Bill: He was arrested walking home from a bar for public intoxication. Now his mistake is to a point unforgivable. Now he has to battle it through to get it expunged.

Frank:
[00:28:00] Yeah, but the problem is just getting it expunged doesn't mean it goes away because you have to remember it may come off on certain websites. In 6 months from now [inaudible 00:28:00] just pops that stuff right back out there. That's the problem with the internet. The problem with the internet is you don't own your own identity. We exist in a society where we're flesh and digital. To a degree we're judged more by our digital life than our real life. Listen, you read about me online. You read all the stuff about me. Nobody has a clue about how my private life is or how I am as a person. To a degree they just see this shady looking character who does this weird business. We as people unfortunately are now just simply judged by the digital.

[00:29:00] I had a girl email me about a year ago. She had a DUI and she was going to law school and she was going to take the Bar. If I'm correct you have to ... Or she was going to law school and she applied to law school. I think you have to tell if you've been arrested when you apply for law school. She was concerned, she found her face on one of those damn mug shots because of a DUI. Here's a young 20, 19, 22 year old girl or whatever she's facing something like this because some website is making money off her. It's horrible. Why should public records ... Why not keep it the way it used to be. You want to know about somebody, go to the town hall and look it up. Everybody wants to make money off your information.

BIll: You go through steps on how to disappear in your book. Do you actually have people that want to disappear? Is there a significant business for that type of work where someone just wants to leave no more traces and just fall off the grid.

Frank:
[00:30:00] Everybody wants to disappear, it doesn't mean they can. You have to figure out how to make a living. I think the majority of people that contact me, it's more of a therapeutic thing. Trying to bang out and figure out their problems. Listen people contact me all the time. I said, "Why disappear just face the music. You're looking to run off into the sunset when you're only going to make your life worse. Disappearing makes sense if you are in jeopardy of a stalker or somebody is looking to kill you. I have this young guy email me he's 21 years old. He got some girl pregnant and he's afraid of how his mother is going to respond and he was going to disappear. "What are you like nuts?" From my perspective I do more these days, I do less of the disappearing.
[00:31:00] I do more of the how do I say this. The digital work, the integrity work with my clients. I work with a lot of wealthy clients who are more concerned how information is connected to them and their family maybe because they happen to be a billionaire and they don't want the world to know they've got a 14 year old child. It can make that child a potential victim for abduction for hire. In a weird sort of way the disappearing has evolved into a business of connections because people think disappearing is not really about disappearing. Disappearing is about avoiding connections, because our whole world is connected and that's the biggest problem we face.

Bill: You know that was interesting because in your book as you moved out of the skip tracing business you mentioned that you mentioned now into more digital dirt. I wrote a note here. I have tons of notes here. I'm trying to piece through as I talk to you. Is it almost the business of disinformation?

Frank:
[00:32:00] It's all disinformation because listen you can't delete anything online. I don't care what they tell you this website will take it off this week, but in 6 months from now or 3 months from now it's just on another website that they own. The European thing. The right to be forgotten is an idiotic thing. You have to remember the only way to combat information is by using disinformation. Take your friends kid with the drunk thing. I would basically be hired to create another individual with his name who takes responsibility for the public intoxication. Eventually when somebody searches online they're going to see these 2 entities your sons friend. Then they're going to see a fake guy who moved to Ohio who takes responsibility for the public intoxication. The only way to ... The whole reputation management thing is ridiculous. It just drives me crazy. It's almost an absurd thing because when you're looking for dirt on someone online you'll find it if you go deep enough. To me it's just about disinformation and deception.

Bill:
[00:33:00] Oh that is fascinating. I see how your business has evolved because you're right. We're totally connected and privacy is complete hogwash right now. It's a hope and a dream you call it. It's almost like the old ancient art of deception and throwing dust in someone's eyes so they can't see. They're blinded to reality.

Frank:
[00:34:00] Planting false flags, whatever it might be. My dear friend Sun Tzu, The Art of War has told it from the year 6 BC. Today, but that's the only answer. Good people do stupid things. Unfortunately today if you do a stupid thing the whole world can know about it and it can ruin your life. What happens is these people end up going to a reputation management company. "Oh we'll fix it. We'll make you look wonderful on the first 8 pages of Google." What about page 13? What about Google images? The reality it doesn't solve your problem. What solves your problem is lying. Lying is a useful tool. Especially when you're combating information that you can't control.

Bill: It's interesting because the things that we did as kids that you did, I did, that we all did in college, high school whatever it may be. That went behind closed doors and it wasn't public, now it's public.

Frank: It's the first time in society where children can see the sins of their parents. Listen, the other big problem is all these newspapers are digitizing all their newspapers so something you did 20 years ago is coming live. We all have skeletons in our closet. There's no conscious on the internet. Nobody cares everybody just wants you to click a Google ad so they can make money off of you. Your life has become fodder for advertisement money and that's it. That's horrible.

[00:35:00]
Bill:
That's the title of this podcast. It's going to be The Sins of the Parents Are Exposed. That's the stunning reality. You know what you're going at it, what I like about how you're doing this Frank is you're going at it with offense. What I mean by that is you're not sitting back trying to ... You're actually going back and leaning into it knowing that you can't change it from the tech point of view. You're leveraging a different strategy, which I ...

Frank: I think I'm very honest about the problem. I don't think that there's a lot of honestly when it comes to what the real problems are online. Nobody likes the fact that Frank Ahern is going to solve your problem with deception. You want to know something? You ain't got no other choice. That's the truth.

[00:36:00]
Bill:
If you want to solve it. For some of the people listening that are running businesses. I love handling this from the personal level because I think once people are stunned into the reality of the personal issues, what would impact their kids and themselves. Then you start thinking, "Well shoot if that can be done personally why it can’t be done at a brand level? At a business level?

Frank: Meaning?

Bill: Meaning if you have a brand impact through a negative consequence through a hack or you're potentially dealing with public disclosure of information that you didn't do. Employees made a mistake or you were hacked or intellectual property or private trade secrets were stolen. Is being able to look at it from a different lens and how can we turn information about this so that the brand is managed better on the down slope.

Frank:
[00:37:00] It's interesting to a point, to a degree. It's almost like the answer to the online is let's develop an app that will solve the problem.

Bill: Because it might not be true. Because what I'm saying is it might not be true. It might be true that the brand had one employee of 50,000 employees that made a mistake. All of a sudden ...

Frank: That is a huge problem.

Bill: One employee then disrupts shareholders, the livelihoods of every other employee that works there. Senior managers. I'm not saying that that person didn't make a mistake, but that the business has some serious consequences as a result of that.

Frank:
[00:38:00] That is a huge problem. One person does something really stupid and the whole organization ... I'll tell you an interesting case I worked on with a client. One of my clients owns a boutique financial company. What happened was a guy, a criminal set up a Ponzi scheme. What happened was he used the same name as one of the employees. He didn't exactly "Steal his online identity." It was kind of similar. When people look up this guy doing this Ponzi scheme they just automatically assumed it was this guy from this finance company. What happened was he ended up swindling these people out of money. What starts happening is they can't find him and there's information generated online. Next thing you know the fingers are pointing to my clients company and this employee of the company.

[00:39:00] Here's a company that's been around for 100 years and never had any problems. The problem is once those few pieces of information go out there it just spreads like wild fire. What happens is most people believe the negative information online, than the true information. They hired me to "What would I do?" I'm more devious. I was like, "Here's what I would do. Why don't we just create a fake identity of who the criminal is. All we know is he used your employee's name. Let's give him a separate identity. This way when people search the internet they'll recognize it's 2 different people."

[00:40:00] They almost kicked me out of this office. I'm like, "You know something this is the best thing I could offer you." They ended up calling me a few days later and said, "You know something? We rethought this, let's do this." Here's what I did. I took what I knew about this criminal. I just started creating a background where he went to school in London. Some family information, some this, some that. What I did was when somebody typed in my clients name, this individual, this employee. They realized there was my client who was the law abiding finance guy. Then this criminal guy from London. It pretty much solved the problem. It''s lying, it's deception. What's the alternative, just keep telling people, "No we didn't do that. No we didn't do that. No we didn't do that." Because that just loses business.

Bill: I know you use the word both lying and deception. It may be a combination of both. A small mistake made by a normal person being amplified and ruining livelihoods is significant. I think it impacts individuals and the business. Again I think some cleverness, deception I think is in order.

Frank:
[00:41:00] Listen the reality is nobody wants to face the fact that the only resolution to the problem might be using deception. They have a huge problem with that. When my perspective is, "You know something? People are just spreading your information which is untrue." What does it matter as long as it gets done. It's a difficult because you have to understand from my perspective any time I sit in front of a client. My answer is, "We're going to have to create deception. This is how we're going to do it." It totally freaks people out. Especially the corporate world.

Bill: Sure.

Frank: It's a huge problem, but it works. I know it sounds crazy, but deception works on the internet today because it's your only tool.

Bill: It's just fascinating. We haven't had guests like you come on and I literally found you through a book I was reading, How to Be Invisible? By JJ Luna.

Frank: I like JJ Luna, it's a good book.

Bill:

[00:42:00] He recommends you at the back of the book. I thought, "God this is just wickedly interesting because personally I think everybody needs to understand this but from the business information leaders, IT leaders, CIO's corporate security officers." I think you've got to understand boots in the ground how this is done. How people, the smartest people in the planet are reverse engineering this problem to still get the outcome. Yes, you can use deception for bad outcomes too. I mean certainly we could have a whole conversation. Someone taking this idea and making it and turning it for malicious intent. I think what we're talking about in the context of this conversation is a good person, a good company, a good employee. The internet being used against them.

Bill:
[00:43:00] Listen, it can destroy a life overnight. Not only that what happens ... There's some people who fell victim where they just shared their name with the wrong person. They were assumed to be the person who committed a horrible act. There's an interesting case in New York with the name Robert Viggiano. Where Robert Viggiano was arrested for trying to have sex with a child. Now ironically in the same town there happened to be 2 Robert Viggianos. Now the one Robert Viggiano owned a plumbing company or something like that. The other one owned a carpentry crew. They have a lot of similarities you want to know that night the news were at the wrong Robert Viggiano's house. This poor guy, people are calling him. Luckily the newspaper did a full page article about him identifying that he was incorrect individual. The problem was the people were posting on Facebook all about him. There's no pulling that back. Some guy was just himself falls victim because somebody else shares the name.

[00:44:00]
Bill:
Stunning, absolutely stunning. This virtual identity that you talk about. I know our conversation has come around from skip tracing to how to this most recent conversation we had about what kind of digital dirt, misinformation. Creating false trails and things of that nature. You talk about connections. Can you explain the concept. Does paying cash for something make you anonymous. Can you ...

Frank:
[00:45:00] No. I define disappearing and privacy as being a virtual entity. Meaning you have no connections to anything physical or tangible. Meaning mobile phone in your name, lease in your name, utilities in your name. You're kind of like a ghost. The way you set that up is either through corporations or other names or other people's names who help you out. Prepaid stiff because information is just information, I explained before. In order for you to be located somebody has to take that information and connect it to something physical, something tangible. That's the connections. Connections are the biggest dangers. Now people think prepaid phones are anonymous and it's not. What happens is they go in.

They buy a prepaid phone in CVS. They walk out and they do their business with this prepaid phone. They totally forget about the physical space that as they made the transaction it was being recorded by a camera. This is one of the problems today. People see privacy as a digital invisible thing, not a physical thing. Even if you're using cash. You walk into a store. There's a connection. You pay for it. There's a camera entering the store. The trick is to not make a connection. Maybe have somebody else go in there. I just want to give you a brief example I tell my clients. Think about it from the perspective of being in high school. You're at a dance, you dance with the bully's girlfriend.

[00:46:00] He's the biggest baddest bully in the world. He's been chasing you around all week with a stick, but he doesn't catch you. Come Friday night you deliver pizza to make extra money. You deliver pizza and you stand outside his house. If you ring that doorbell he's going to open that door and he's going to beat you with a stick. If you go back to the pizza shop without delivering the pizza you're going to get fired. What do you do? You take a ride down the block and you find another teenager. "Hey you want to make 5 buck? Go deliver this pizza. Get me the money, keep 5." They do that you take the money back to the pizza shop. The bully's got his pizza. The pizza shop has got its money and you've got your teeth. That's avoiding connections because if you would have rung the doorbell you would have been captured. The disappearing is really not about disappearing, it's about avoiding connections. That's how I explain disappearing.

[00:47:00]
Bill:
It's a ghost. Now it sticks for me. You become like a ghost because nobody can physically pin you to a location.

Frank: Right, but you did what you had to do. You obtained your objective, but you did it without being connected to it. That's the idea. Connections are the thing. Disappearing starts with dreaming, most people. They forget. They forget that they're sitting at home and they're typing in Cayman Islands or their work and they're typing in banks in Belize. Next thing you know they disappear to the Cayman Islands a year later. They've already created the connection with the Cayman Islands, the digital footprint. It's like the guy who kills his wife and a month before you see him at the hardware store buying a buzz saw. He's on camera. That's a connection. You're creating these connections. Be it physical or be it digital. That's how I view disappearing and view what you must avoid in life and remain disappeared or private.

[00:48:00]
Bill:
Some people think that the lack of privacy will lead to a better society at some point because everybody will double check their actions before they act. I'm not sure I believe that, but it's an interesting perspective.

Frank:
[00:49:00] No. I think we as humans have our flaws. We're still going to do what we're going to do. We're going to try to be discreet about it, but listen we still make mistakes. I think it's more to the perspective that we're in a society where they expect you to have less faults because of that. Humans are humans and we make mistakes. I think hopefully that in time the internet will probably change. Meaning I don't think it's going to be this thing where there's a ll these database sites. They're talking about getting rid of and passing a law against these mugshot sites. They're just predatorial. I do think as time goes on, I do think the internet will mature. We won't be such like a wild west of information.

Bill: I agree with that. I think the debate on ethics. The debate on privacy. The debate on what's right. The technology has a certain pace to it now. It's interesting this is a great metaphor that I learned the other day. You can steal it if you want from me. If you like it. When the car was invented in the late 1800's seat belts were a good idea then when it was invented. The actual mandate of seat belts didn't happen until the 70's.

Frank: Interesting.

Bill:
[00:50:00] 90 years later. It wasn't mandated everywhere in the world. It was only mandated in front seats, not middle and back seats. It's interesting and not on car seats or kids, small kids. It's interesting seat belts on the internet. Seat belts are a good idea now.

Frank: Exactly.

Bill: Now, but when we're going to have seat belts, I'm not sure.

Frank:
[00:51:00] That's a valid point. I think that's the exact same problem with the internet. We know what should and shouldn't be. We know what should and shouldn't be with privacy. Hopefully at some point there's an evolution and government says, "You know something, maybe we should do right by people and change or companies themselves embrace the change. Spokeo is there really a need to have a company that exposes your regurgitated information? Your age, your past address. What's the point? When I find people I'm very cautious who I do business with. You just can't be Joe Blow and hire me to find someone because I know there's a responsibility to it. You can hurt that person. I don't know I just think that there could be a change in the future.

Bill: From the people listening here as we start to wrap up Frank. What is the top question you get asked by either in your seminars or one on one conversations. What's the top question right now?

Frank:
[00:52:00] Can you disappear in the age of big brother? That's number one. My answer is yes. Data, technology, information is like food in the refrigerator. A human being still has to open that door. Take out that information, send it out to the world. A human being and the best example is you take facial recognition in London, most amazing system. A criminal walks down the street a face comes on the computer. You still need a the human to run out there and capture the person. Right now technology needs human. That's going to change when Robocop comes along though and it's coming. It's always ... That's the biggest question can you disappear in the age of technology, big business, big data, big brother?

Bill: In your book you go through how to do that. You when I asked that question earlier you more often find that people when you hold their feet to the fire on that don't often go down that route. Is that what you see most often or do they actually ... Do you have a good chink of people that do want to disappear or does it turn into more of a disinformation effort?

Frank:
[00:53:00] It's been more the direction I want to go in. Dealing with people who want to disappear is sometimes a nightmare. It's something that ... I did it for quite some time. It was really cool. It was really exciting. I still do it once in a while. I take one case a year that's all I need. I'll do maybe one person a year. It's just a question of ... 99% of the people contact me. "Frank listen, I need to disappear. I need a new identity and I need a new passport." I'm like, "Yeah, no problem. I'm going to get you the Harry Potter invisibility cloak as well." It's a crazy business, 99% of the people that contact me I'll never do business with. I just need that 1%. That 1% can be one client.

Bill: I think everybody kind of has the Jason Bourne thought when you disappear to that island after he went through that whole issue. They still found him there.

Frank: Exactly. Just because you want to disappear doesn't mean you can. Nor does it mean it's the smart thing to do. Sometimes you've just got to face the music.

Billt: It has to be the 1% I guess because you mentioned the 3 questions you have to ask are, where do you go? Is it safe? Do you have living money? You have to be able to live comfortable with as much cash as possible because you don't want to be ...

Frank:
[00:54:00] You've got to be able make money and not be traced to your money. You can't commit tax evasion. It really depends. Everybody has what I call the palm tree lifestyle, the palm tree dream. Everybody wants to go to the beach, live under a palm tree and drink pina coladas. What they don't realize is it's expensive to live at the beach. I have people contact me. I had this one guy contact me, it was really horrible. He's getting $500,000 buyout from his company. He just wants to disappear on his wife and kids because he hates them all and they hate him. That's so vacant. I said, "You're 30 years old that 500 grand is not going to last you the rest of your life. What are you going to do when it runs out? I said why don't you just give your Ex half of it and go disappear and live in Iowa or something like that.

Bill:
[00:55:00] I love this concept. What I learned from this conversation is that it doesn't have to be about disappearing. It's like being a ghost and being less visible, because in your book you talk about even going through the EZ Pass. Through New Jersey and Massachusetts and New York. You've got GPS's on your phones. We still have to live life. It's almost ... Your comment earlier was just be aware of where your digital footprint is being left behind.

Frank: Exactly. I had a client meet me once he pulls out his phone and checks his email. I'm like, "Are you dumb?" The GPS shows you're sitting here with me right now. The disappear book is still a really good book. How to Disappear. It's got a lot of information. I've changed my perspective these days of what and how to disappear actually is. Environment is the key. How do you get from point A to point B?

Bill:
[00:56:00] I really really appreciate this conversation. I do encourage everybody. I'm not going to read through the list of books again because we did that in the beginning. I do encourage people to go out and read your books and understand. What else are you doing Frank? How else can people learn about you? What sources can people go to engage with you or talk to you or just learn about your work.

Frank: They can go to my website disappear.info and engage just drop me an email and say hello. See what happens from there. I'm not involved with any social media or anything like that. I'm always open to talking to people.

Bill: Just good old fashioned email if people want to reach out. There's no necessarily ... They don't have to talk to you on LinkedIn or Twitter. If they want to talk just to get [crosstalk 00:56:32].

Frank: They won't find me on LinkedIn or Twitter. To me I don't understand that either why not just email someone. Isn't that the purpose of email is to contact them?

Bill: It is.

Frank: Just email ... Why do we need other ways of contacting when It all comes back to our email anyway?

[00:57:00]
Bill:
It's funny people say that email is disappearing, but it is absolutely not. People set up Twitter accounts, LinkedIn accounts, Snapchat. All of these services push people back to either a gmail, a yahoo, bing or their company email.

Frank: Exactly. Why not just email me if you wanted to say hello. That's just my philosophy.

Bill: Is there any book you recommend to people? It doesn't have to be in your particular line of work. Is there any book you found most helpful and useful for yourself that you could recommend for others or share the name of?

Frank: You know what to be honest with you. I read a lot of French literature. I don't read books about privacy or techno or anything like that.

Bill: Did you say French literature or fringe literature?

Frank: French literature.

Bill: What do you ... Give me an example.

[00:58:00]
Frank:
In Maupassant Lola just ... People always say, "What's your favorite mystery book?" I'm like, "I hate mysteries man." I've just always been a huge fan of literature, especially French literature. People always find that weird. Listen I deal with mysteries and garbage and dismal and horrible stuff daily. Why do I want to read about it at night.

Bill: What about French literature. Tell me about that. I'm just not as familiar. I'm just very curious from my own personal interests. What is it about French literature that's appealing?

Frank:
[00:59:00] It's beautiful writing. I love even Camus stuff, some of Sartres. I don't know I just always had this affinity for French literature for some reason. It used to be Russian literature, but after a while it gets a little tough to read. French literature to me just works. It's relaxing.

Bill: Afterwards I'll email you and maybe you can just send a couple of titles and I'll put it in the show notes. I'm going to put on this on our conversation on the show notes on the RedZone Tech.net/podcast. I'll pout links to the books, links to some of the writing you like. Links to the show.

Frank: One quick point. It's interesting you talk about the books because people see me and they think I live and breath this disappear and privacy stuff. Some people think I'm technical. I am far from technical. It's all about perception. That's what happens on the internet. It's just perception until proven otherwise.

Bill:
[01:00:00] That's interesting because you would never pick up that from your day to day mask. Your day to day persona. We all have masks, right? We never really know what's behind the mask until we ask. It's not necessarily going to be there.

Frank: Exactly.

Bill: Interesting. This is fascinating. I really appreciate you for your time Frank.

Frank: Hey, thank you I really appreciate it.

Bill: This is a lot of fun. This is massively interesting. I'm sure people that are listening are just going to be super thrilled. I hope we can do a round 2 at some point.

Frank: Anytime man.

Bill: Okay. Thanks.

Frank: Have a great day. Thanks a lot.

Host: You too. Take care. Bye.

Frank: Bye.