When it Mattered

Episode 9: Bryan Cunningham

Chitra: Hello and welcome to When It Mattered. I'm Chitra Ragavan. On this episode we will be talking to Bryan Cunningham. He's an international advisor to companies and governments about cyber security law and policy, emerging technology, surveillance and privacy issues. As a senior CIA officer and federal prosecutor, Cunningham worked closely with the 9/11 Commission and provided legal advice to the President, National Security Advisor, and the National Security Council in the Bush and Clinton administrations. He was a principal contributor to the first national strategy to secure cyberspace. Bryan, welcome to the podcast.

Bryan: Thank you. Thank you for that generous introduction. Another way to think about that as I can't hold a job.

Chitra: Well, you have been a globetrotter for the past decade as an international man of mystery and cyber security expert. I usually catch you at airports between flights, but where are your roots?

Bryan: They could not be more Norman Rockwell. I grew up in a small town in northern Ohio population 12,000, give or take. My father was an Episcopal minister in this little town and my mom was the librarian. So it was very Norman Rockwell. But as behind every Norman Rockwell painting, there was a lot of undercurrent that was happening in the town. There's actually a novel by Sherwood Anderson called, Winesberg Ohio, which a lot of folks read in middle school and it tells the behind the scenes story of one of the small towns and all the crazy stuff that was going on and that real town was about 30 miles away from the town I grew up in. It's not actually called Winesberg, but the book is fairly accurate about the kind of emotional and small-minded stuff that goes on in those little towns.

Bryan: And I was a bit of a victim of that when I was about 12 or 13, we lived in a wooden house rectory provided by the church and my dad was somewhat controversial. He had a large parish in Cleveland a few years before this, invited Dr. King to speak from the sanctuary and he didn't get the permission of his boss at this very white, very conservative church

and so he suffered a lot of repercussions for that. And eventually, the Bishop sent him to the small town in Ohio, where he continued with his agitation for race rights as the locals would have called it, his agitation.

Bryan: So there was a lot of scrutiny on him in this small town. And when I was 12 or 13, our house burned down, burned to the ground. And the local newspaper, without any facts, reported that the cause of it was children playing with matches. And even though I wasn't home at the time it happened, my younger brother was way too young to have been the person and my older brother was in college. So, then I was that, I was the person and the whole town assumed that, and believed it, and really made my life difficult for the rest of the time I was there. Fair amount of bullying, a lot of undercurrent of attacks and things like that.

Bryan: And so that was a very formative experience in the sense that in a little town like that, when you get tarred with something like that, very difficult emotionally, I can't even imagine what it would be like now with social media, not sure I would have survived it. But I did two things that really sustained me for the rest of my life. One was I started playing the drums and I was able to lose myself in music and that also turned me to a whole nother circle of friends and acquaintances that weren't part of the little town system. And every time in my life that I've had a dark moment, that music has been able to help me get past that. And then the other thing is, I learned that you can be the victim of something very bad and very painful, and it will pass, and you'll get through it, and you'll be able to move on.

Chitra: And how did you move on? What did you do next?

Bryan: Well, I started playing drums professionally at age 14 and that occupied a lot of my time, and also made me some money because my parents had almost no money. So I was able to take myself to the University of Colorado as a freshman and paid for it myself. And then during that time, I applied to the Iowa Fiction Workshop in Iowa City and transferred there, did my last two years there, that was another very formative event. That was probably the most important professional development thing I had done because it really teaches you how to get the ego out of your writing and anticipate what the reader is going to be thinking, it makes you a much better writer, also got me a lot of job interviews. But that is the second thing, fiction writing that has sustained me through all of difficult times I've had. And as I've been thinking back on my life so far, it occurs to me that even though I've been all these other things professionally, and I've never been a full time professional writer or musician, that's my roots. I'm an artist at heart, I think.

Chitra: So how did you end up becoming a lawyer in a big firm and then government?

Bryan: Well, at the University of Iowa I was destined to have a fiction writing degree. And as my girlfriend's father said at the time, a fiction writing degree in a dime will get you about 10 cents. And so, I went on exactly two job interviews at the University of Iowa in my senior year. One was with an insurance company and the other one was with the Central Intelligence Agency. And I had always wanted to travel and do government related things, but honestly it was more that those were the two interviews I got. And so when I graduated, I had no job, and I went to work on a senate campaign, congressman from Iowa Tom Harkin was running for senate, I worked on his campaign. I believe we were paid $400 a month out of which we had to take our own expenses. And he got elected and I was one of the 10% of the staff that got to go to Washington with him. So I became one of his aides in the Senate.

Bryan: Then 18 months after the interview with the CIA, they called and said, "We'd like to put you in our career training program." So I did that and I was a career trainee and then, this is how long ago it was, a Soviet Foreign Policy Analyst. And I actually thought those skills would never come in handy again, but now with Putin, I'm thinking maybe they might be valuable. And so I was there, I got a little bit disillusioned by Iran Contra, for those of you who don't remember that, it's easy to look up. And I left and went to University of Virginia law school in 1987, graduated in 1990, clerked for a federal judge in San Francisco, went to practice law in Colorado where I had my law license, and then when President Clinton got elected and appointed James Wolsey as his Director of Central Intelligence, a law partner I had worked with that a firm before called me and said, "Hey, I know Wolsey, you should come back." So then I went back to the CIA this time as Assistant General Counsel.

Chitra: And then what happened after that?

Bryan: So that was 1994-95 and I worked as Assistant General Counsel for most of that time although I got to go try big drug cartel cases at the Department of Justice. And then towards the end of my time, in that iteration of my CIA career, I was the executive assistant to the Chief Operating Officer. So that was a purely policy operational job, it was not a legal job. And that was actually quite valuable as well because it allowed me to be inside the head of my clients as a lawyer because I got to, at point, supervise lawyers, not be one and it really, I think, probably made me a much better lawyer.

Bryan: And then I left in 2000 because by this time we had one daughter and one on the way and government salary wasn't going to put them through school and college. And so, I went to a big law firm in Washington and that was the second time I told my wife I was leaving the government never to return, and then 9/11 happened. And so, when 9/11 happened, we were living on the flight path into the Reagan airport, we actually heard the plane go into the Pentagon. And I just felt having been a CIA officer and a national security lawyer, I should do something to contribute more than just giving blood and money, so I started looking around for another national security job even though I knew, and my wife knew I was going to have to take a two thirds pay cut to do that.

Chitra: And did you get the job that you wanted?

Bryan: There's a country song lyric, thank God for unanswered prayers. And the answer is, I did get the job I wanted ultimately but not in a very direct road. What happened was, I got recruited to be a lawyer on a congressional committee that was looking into some things related to 9/11. And through a whole series of unfortunate political machinations that were more about the Democrats and Republicans fighting than about me personally, I got the job, and then before I ever started, I lost the job. And I was devastated. I thought, boy, I really want to be contributing, this was the perfect thing, and now how am I going to make a contribution.

Bryan: But what happened was, the person who ultimately got that job that I didn't get, left the job as the Deputy National Security Advisor to the National Security Council and the White House and then they recruited me to take that job, which was a far better job and really has defined my career ever since.

Chitra: So in a way, that setback really paved the way for your future career.

Bryan: Absolutely. But as I've been thinking through all these events and how they tie together, the early experiences I had with the small town and having to overcome that made me realize that even though I lost that one job, if I had just persevered and try to keep a good attitude, likely something else would come along, which it did. So it worked out.

Chitra: And then you are now a cyber security expert and you got into it at a time when nobody ever was really even serious about it.

Bryan: Yeah, I had done some legal compliance work at the big law firm before I went back into government. And then at the White House, I was, as you mentioned, one of the principal authors of the first national strategy to secure cyberspace which necessitated all of us working on that

document to really teach ourselves cyber security because really, there were some folks practicing cyber security but it was very obscure discipline. So, when I left, having gained all that knowledge and experience, I thought, be great to go out and practice cyber security law, but what I quickly found out is there was no such thing as cyber security law. Really, I'm sure someone who's listening to this podcast will write in and say, oh, I was doing it in 1999, but I couldn't find anyone doing it in 2004.

Bryan: And so I did a bunch of research, I made a business plan, I took it to all the large law firms that I had ever been affiliated with, and none of them wanted to touch it. They all felt like it wasn't going to last, first of all, and then the bigger impediment was, I felt like it was important to try to do that on a fixed fee basis as opposed to just charging clients an hourly rate forever, and none of the firms wanted to do that. So, I wound up just hanging out a shingle and moving back to Colorado, and proselytizing cyber security law, speaking at conferences, writing legal and ethics chapters in IT security textbooks, and no one paid me to it at all. I did other legal work that paid the bills, but nobody wanted to pay for that.

Bryan: Then California passed the first breach disclosure law, thank you California, and a company called ChoicePoint had to pay massive fines. And now all of a sudden, two and a half years after I started thinking about it, people wanted cyber security lawyers. And if you had googled, cyber security lawyer at the time, I would have been one of five or six people that you would have found. So, that was just off to the races. And I had been practicing cyber security and privacy and data protection law ever since, in one form or another, and that has also led to things that were unexpected like being invited to Cound and be the executive director of the first Cyber Security Policy and Research Institute at the University of California. So, I'm one of those people now who has three or four jobs, but all are related to cyber security in one way or another.

Chitra: I guess taking that risk actually paid off in a big way. But at the time, it must have been scary.

Bryan: It was. You know very well what it's like to start a new business. And in 2004, there was also no science of being an entrepreneur either. Now, people can hire you, people can read books, people can watch videos. The only real rule I was able to find out is, if you want to start a new business, you need to have six months worth of savings to cover all of your expenses. And so it was scary because my daughters were seven and five, and we were moving to a new place, and I had no guarantees at all that I would get any work much less cybersecurity work. But again, I guess these experiences of having things look somewhat hopeless and

persevering, and then having things work out, I just believed it. And I just believed it long enough it'll work. And since then, I've started two other law firms and a consulting company and a cyber security Institute and it's always the same, you always have uncertainty, it's unclear whether you'll succeed at all, and it's very unclear whether the business you thought you were founding is the one that you'll wind up with.

Bryan: And then of course, you have the dilemma when you get a little success of, how much work can you take on, and do you need to expand and hire people? And I at least feel a lot of personal responsibility for someone, if I hire them, I figure I have to now generate the work that's going to support their family and I'm sure they have their own economic issues. So, that's an ongoing dilemma. But what I've tried to do is create enough different jobs, different income streams, that if any one of them falters, the other ones will be there to pick it up. And so far, so good.

Chitra: And looking at the landscape now in cyber security, it's completely transformed as you know and I think the American public and much of the world is already now still digesting the impact of the Russian interference in the U.S. Elections, and you see North Korea, you see China actively attempting on a 24 hour basis to penetrate our cyber security. What are the biggest changes that you've seen since those days when you couldn't get anybody to hire you for this?

Bryan: I always tell my cyber security clients that there's two kinds of companies. There's the kind that know they've been breached, and the kind that don't know they've been breached. And it's a little bit of an exaggeration and actually, I might have stolen that from your prior guest, James Comey, but it's true at this at a certain level. And the truth of it is that, there are hundreds of thousands, millions of attacks being launched every minute of every hour of every day. One of my law firms represents a client that the Russian government is not super happy about. And so we get tens of thousands of attacks every day and they're very sophisticated, and of course, being in the cyber security business, we're able to get the right kind of controls in place, and hire the right consultants, and so far knock on wood, there haven't been any successful attacks.

Bryan: But on a broader level, I think the next phase of this is going to be our reckoning with the fact that we are really are in a perpetual cyber war. It's just we're not fighting it. The Russians, and the Chinese, and the Iranians, and others believe that stealing intellectual property, disabling systems committing ransomware, blackmailing people, hacking elections, are legitimate uses of national power. There are thousands and thousands of individuals in Russia and Ukraine and probably millions in China, who

literally go to work every day, punch the clock and sit there all day and take their orders and try to hack into Western systems. And they don't think that's a problem. That's part of their economic plan and part of their military and diplomatic plan.

Bryan: What I think is changing right now is that there's starting to be a broader awareness that this is happening. And the lines between government action and private action and war are getting very muddy. So I give a talk regularly to cyber security professionals. And I talk about the fact that 90%, 85% of all the critical infrastructure in the United States is owned by the private sector and defended by the private sector and yet it's being targeted by these other governments as though the private sector were a government.

Bryan: So, for example, I was an expert witness last year in a big litigation involving the North Korean attack on Sony in 2014. And if you think about that, North Korea essentially treated Sony like they were another government with whom they were at war.

Chitra: The issue was Sony had released this movie, The Interview, which was a spoof on the North Korean dictator.

Bryan: Right. One could argue they just can't take a joke, but I actually think it was a lot broader than that. I think that the North Koreans wanted to stop the movie from being released, but more importantly, they wanted to find out if they could actually coerce a Western company into doing what they wanted. And so, they committed acts of war, if those had been committed against the government, they would have been acts of war and under the laws of war, if you attack a private entity in a country that has military consequences can still be an act of war. They committed espionage against them, they extorted them, or what we would call it polite circles, diplomacy, when a country puts sanctions on another country to get them to not do something, that's called diplomacy. This is what happened to Sony from North Korea. They locked up their data, they threatened to release it unless Sony complied with their demands and ultimately, they did release all the data. So then that was creating massive economic damage.

Bryan: Well, so how does that fit into the rules of nation state conflict? We would have had the right, under international law, and President Obama actually at the time said that, to have retaliated with cyber force or actual kinetic military force guns, missiles, bombs, when a cyber attack reaches a certain level. And I think it's just inevitable that will happen. And I actually think one of the big mistakes that President Obama and President Trump have made, is not sending a sufficient signal to Putin and all the other

dictators around the world that there will be consequences for things like trying to influence our elections.

Bryan: Reportedly, we have now finally sent the message to Moscow that we have the capability to cripple their electric grid and we will if they continue to mess around. I don't know whether that actually happened or not, and I don't know what level it takes to punch back against a bully like Putin to make him change his ways. But one thing's for sure, if we don't do anything, they're just going to keep pushing as hard as they can. And I still don't think we're at the point yet where enough people in the population view it as a national security, economic security, we're all in this together prepare for warfare situation.

Bryan: So when I give this talk, I liken our current time to the times of the East India trading company and pirates and privateers, where governments either cannot or will not protect the infrastructure of the country, which is in the hands of the private sector. So, to some extent, the private sector has to get together and defend itself. And the other metaphor I use is Dunkirk. So when the 400,000 or however many there were British army were pulled off of the beaches at Dunkirk, of course, it wasn't by the British Navy. It happened because the British government said, "Hey, anyone with a sailboat, or a fishing boat, or a yacht go across the English Channel." Think about that, they went across the English Channel into enemy fire completely unarmed, no military training, and rescued the soldiers off those beaches and arguably prevented Britain from being completely defeated by Hitler.

Bryan: And so what I say to these cyber security professionals who are often underfunded, and overstressed, and beleaguered, and somewhat depressed, I say, hopefully, without too much melodrama that, if we all do our part in shoring up all of our individual cyber security systems, we actually might save the world.

Chitra: But that's easier said than done because it seems that the public is somewhat numb because there are these massive breaches, the most recent being the settlement that Equifax did with hundreds of millions of dollars, and you had the breach against Target. And so I think, for a lot percentage of the population, there's already the belief that there is no security, there is no privacy, that the data is already out there. So is that true and how do you convince people?

Bryan: Yeah. I think there's a certain amount of numbness. I mean, I'm in the business and I get two or three notifications every month that there's been some data breach and really, I don't do anything about it, I feel like I've already done a lot to protect my own security and those letters now

just are like junk mail. And part of what's not happened yet is our legal system imposing sufficient enough damages on most companies that they'll actually change their behavior. Let's take Equifax for example, they did pay a massive fine and there have been other pretty severe fines, but that should have been a bet-the-company proposition because here you have Equifax who not only hold some of the absolutely most sensitive data about hundreds of millions of us that could possibly exist, but you would think that they would therefore be at the most heightened security of any company or any type of company other than health care, or bank, or something like that. They were pretty easily defeated by a relatively unsophisticated attack and I really felt like they would go out of business because you have essentially three credit reporting companies, they all charge almost the same amount, it's really like a commodity.

Bryan: So, as a consumer or a business, if you're going to pick between one of those three, and they all cost the same, and they're all basically equally helpful to you, why would you spend any money with Equifax? Why wouldn't you go with the other two? But hasn't happened. People have not massively switched away. I still go to Target. I never stopped going to target. So there is a psychological barrier to the public getting sufficiently outraged, or afraid, or cautious. Now I think that's going to change though because up until now, most cyber breaches have been primarily economic, not exclusively, but primarily economic, stealing information because of the information's value, stealing credit cards to use the credit cards.

Bryan: And again, like I said, people have become numb to that. But the next phase of this is going to be, I think, much more malicious and impactful ransomware. Ransomware, as you know, is where an attacker will get into your computer system and encrypt all of your data in a way that you can't use it and then either make you pay, usually Bitcoin, to get the data back, or if you have sensitive data that you're embarrassed about, like Sony had, they'll threaten to release it unless you pay them a certain amount of money. That's a pretty esoteric attack, it doesn't happen to that many people, and also, again, it's just money for the most part.

Bryan: The next generation of ransomware is going to be what is starting to be called hackware. And what hackware is where they seize and take control of Internet of Things device, not just a computer. So think about all the systems on your car that are connected to the Internet. There's already been at least one attack in Austria where the attackers were able to electronically lock all the doors in a hotel. And in that particular situation, the engineers in the hotel were able to get people out but imagine if they did that to a nursing home and turned up the heat to 110 degrees or something, or this has happened in hospitals already -- they've had their

surgical record and some of their devices locked to the point where they couldn't perform surgeries.

Bryan: When you start getting a massive scale of people's cars being stopped on the highway, or people's surgeries being messed up, or God forbid, somebody die or it's the air traffic control system, or the energy grid. Unfortunately, I think something like that is inevitable and that is when I think we'll wake up more as a society and decide to be more willing to do collective defense like Winston Churchill once said about America, you can always count on Americans to do the right thing after they've exhausted all other options.

Chitra: But do you think that the U.S. Government is prepared for that level of threat?

Bryan: I haven't had a security clearance since about 2009, so I don't know. I would hope that we are much better prepared and much better at this than it seems like we are. Again, I'm certain that both the Obama administration and the Trump administration have the tools to do much more damage to another country than we've ever been willing to do that we publicly know about. And I'm not particularly in favor of offensive cyber warfare, but I am in favor of making the Chinas and Russias of the world know that we have the deterrent capability to really cripple them if we need it. And sometimes, to do that, you actually have to show them that you can do it.

Bryan: So, I think we have the tools, I think we still, in the United States, have the best cyber warriors in the world at the National Security Agency, at Cyber Command, and the other areas, the military and intelligence community. I just think so far, as far as we know, there hasn't been the political will to use that capability. Now, on the other hand, if the question is, is the United States government prepared to defend our energy grid, to defend our air transportation system, to defend our automobiles, and to cope with the aftermath of a successful attack? The answer to that is, I don't think so at all.

Bryan: And part of the reason is they can't be because, as I said, so much of the infrastructure is owned by the private sector. And unlike in a country like Russia, or China, or even a more democratic country like Lithuania that doesn't have the constitutional protections that we have and the culture of freedom and openness that we have, we're not willing to allow the government to do what they would have to do to really protect the infrastructure. And that is, put government military intelligence or law enforcement sensors, devices, and operatives into all of these private

critical infrastructure systems. We just are not willing to accept that as a country, at least not until something catastrophic happens.

Bryan: Now, Lithuania, or maybe it's Estonia, one of the countries in southeastern Europe has what I think is a great program, which is it's essentially a Cyber Security National Guard. So, those countries have been beaten down by Russia over the last 15 years. Estonia almost got their entire country shut down for a couple days. So what they've done is they've created a quasi-military organization where cyber security experts and information security officers at many of their most important companies also are in the Cyber National Guard. So they go for training for a couple weeks a year, they put a uniform on and go, they go serve weekends. And then if and when there is a real emergency, all of those people will get immediately activated to active military service. So now, you have the people with the knowledge in the right positions in the private sector, able to become a defense force in an emergency.

Bryan: Again, I don't think our cultures, and our traditions, and our laws are prepared to have that, at least until there's some kind of, hate to use the phrase, but cyber Pearl Harbor. And I do think something like that is coming, it's just inevitable and it's like with terrorism, we have to be right 100% of the time and they only have to be right once.

Chitra: Well, you've got a lot of these very scary ransomware, and these attacks, and things like that, but on the more seemingly benign, just to, it's not the right word, but you've got things like the recent scare over Face App and whether that aging app was actually sending data to the Russians. And you got these plug-ins that are extracting data while you sleep and and using them for getting more information about you to the advertisers. What do we do to educate people about that, and is that also a level of threat that we need to deal with?

Bryan: Yes, the first thing is getting people to care because the actual cyber hygiene measures that every one of us could be taking to prevent a lot of these attacks are quite simple and easy to use. It's just this numbness that I've referred to before where not that many people have seen direct, horrible consequences happen to them, and it's almost like now we're in a boy-who-cried-wolf situation, we're getting warned about so many things all the time, that we don't know which ones to pay attention to. But, free advice for your listeners, if you do just a couple of things, you're going to be quite safe from most types of attacks. The most important single thing to do right now, in my opinion, is and of course, I can't give legal advice over a podcast, but just as a tip is to get multifactor authentication on every email account and every important account that you have.

Bryan: And nowadays, your banks are really forcing that on you. So Wells Fargo, you try to log in, It'll want to text your phone. That protection imposed on email systems and all of your other systems will prevent a huge percentage of the attacks. Then, most important thing, just do not go to websites or click on links that are in emails or texts from somebody that you're not certain you know are sending it to you. I run the Cybersecurity Institute at UC Irvine okay, yesterday in one day, I got two different what are called phishing emails that had the University of California Irvine IT department logo on the top and it's kind of diabolically clever. There were two versions of the same thing. They both said, we've had an information security incident, your email is not secure, click here to get it back to correct security. And of course, they were phishing attacks. If I had clicked on either one of those I would have had my phone and ultimately probably my computer infected and they're very sophisticated.

Bryan: I've had phishing attacks where it looked exactly like it came from my wife at the time, I've had a text that purported to be from a speaker's bureau that wanted me to come on as a client and the scary part of that was, they actually quoted me from a speech I had given a year before that was not public. So I don't even know how they did that, and I didn't click on it because I'm in the business and because I also thought, a speaker's bureau probably isn't going to contact you that way. But if I didn't know better, I would have, Why wouldn't I?

Bryan: There's a version of this where these emails claimed to be from the FBI asking for your help in catching a cyber criminal. I mean, they're very, very clever. But if you do those two things, multifactor authentication, and don't click on links or go to website URLs that are not certain to be from somebody that you know and trust, that's going to solve a lot of the problems. Oh, and of course, ransomware. The current ransomware, not that future hack where I'm talking about, but the current ransomware where they just want to lock up your data and charge you to get it back, that is 100% preventable. And that is just by backing up your data to another device that's not connected to your computer. So, just get an additional hard drive and backup your data every so often and then if they hit you with ransomware you say, sorry, I got other data, go away.

Chitra: Yeah. It's just a whole new world and it's interesting that you're in this space and you're also an expert on privacy, looking back at kind of your 12 year old self dealing with that fire, and the issues that you dealt with, and the sheer loss of privacy in a small town, do you think that impacted course of your career?

Bryan: I hadn't actually ever thought about it that way. But looking back on it, that's probably right. It probably happened in a couple ways. One, I

developed a deep empathy for victims and so I've done things like been a Pro Bono general counsel to the largest anti-human trafficking organization in the country. A lot of what I've done in law enforcement and intelligence and national security has been trying to protect people from being bullied, whether it's by countries or by criminals. And I have consistently, in every job I was in, gravitated to parts of the job that involved privacy and protecting privacy. So I had not actually thought about the connection, but it's probably right.

Chitra: And in this age of social media, it just seems like a lot of us have already accepted that we don't have any true privacy, not does for instance the younger generation seem to even care that much, because of this free flow of information. So it opens the door for a lot of vulnerabilities.

Bryan: Yeah. As a society, we're willingly and enthusiastically rushing into giving up our privacy and our data. People will allow Starbucks to do almost anything as long as they get a text that says, you got a free coffee coming. Kids, in order to be followed and popular on social media will reveal, and not just kids, adults too, will reveal much, much more information than they should. And I think some of it is, the two generations behind me, my daughters who are 21 and 18 and their generation just don't think of privacy the same way that we did. And some of it is, again, that the value systems, I sound like an old man now, but the value systems have changed to the point where it's more important to the younger generation and to a lot of adults, to be popular online and be seen as living a life that other people will want to follow, to be interesting, that's more important to them than privacy.

Bryan: A great story, horrible story, but illustrative. About four years ago, the British Secret Intelligence Service had appointed a new director, so this would be M in the Bond movies. And historically, that person's identity has been secret. So the Bond movies calling the person M, that's a real thing, it came from the real British Secret Service, they used to call the person C, I guess, for Chairman or something. And in more modern times, it's not as secret as it once was, but you can't have a head of the British Secret Intelligence Service with their public public data, including their address and things like that.

Bryan: So a man got appointed to be the next Director of the British Secret Intelligence Service and his wife had a very significant Facebook presence. She'd sort of documented everything they did on their family including a lot of information about travel, like where they're going on vacation, got pictures of their kids up and things like that. She posted, I'm so proud of my husband for being the new head of the British Secret

Intelligence Service, and he lost that job. He was never able to take that office because of that.

Chitra: That's an incredible story.

Bryan: Yeah.

Chitra: Wow, this has been a great conversation. Do you have any closing thoughts?

Bryan: I would just say, well, first of all, thank you for the opportunity to do this. I would just say that in thinking back over all these events to prepare for this, I'm probably repeating myself, but just to crystallize it, I really appreciate now the power of the arts in one's life even though that's not necessarily your profession because, as I said, in good times and bad, I've always been able to turn to music and writing as kind of almost self-therapy. Not to mention the fact I put myself through law school playing drums, so it has practical benefit as well. And then the other big lesson is just, it's a cliche now, but sometimes adversity is the best thing that ever happens to you. The other thing that happened to me because of that incident with the fire and the way I was treated is, it just made me much tougher. It just made me much less susceptible to bullying and to attacks because I suffered for a number of years, but then I saw that I was able to get past it. And so after that, I was pretty resilient.

Bryan: And so sometimes, the worst things that happened to you are the best things that happened to you.

Chitra: Great. Bryan , where can people learn more about you?

Bryan: Well, the Institute that I run is called the Cybersecurity Policy and Research Institute, it is at cpri.uci.edu. One of my law firms is Cunningham, Levy, Muse our bricks and mortar headquarters are in Washington, DC. And we do lots of other things, we do, besides cyber security and privacy law, we do Congressional investigations, defense, white collar defense, I have a bio there and if we can help folks, I'm happy to do that.

Chitra: Great. Thanks so much for joining me.

Bryan: Thank you.

Chitra: Thank you for listening to When It Mattered. Don't forget to subscribe on Apple Podcasts or your preferred podcast platform. And if you liked the show, please rate it five stars, leave a review, and do recommend it to

your friends, family and colleagues. When It Mattered is a weekly leadership podcast produced by Goodstory, an advisory firm helping technology startups find their narrative. For questions, comments and transcripts, please visit our website at goodstory.io or send us an email at podcast@goodstory.io. Our producer is Jeremy Corr founder and CEO of Executive Podcasting Solutions. Our theme song is composed by Jack Yeagerline. Join us next week for another edition of When It Mattered. I'll see you then.