meetinnovators™
where the deals get done

Interview with Jon Praed from Internet Law Group

Adrian Bye: Today, I'm here with Jon Praed from the Internet Law Group. Jon's a pretty interesting guy. This is the interview I've been looking forward to handling for awhile. Jon is someone who's spent a lot of years tracking down hardcore internet spammers and bringing them to justice. He does it on behalf of companies like Verizon and AOL, and has won some pretty important lawsuits and some decent-sized judgments. Jon obviously has some strong opinions on this space as well as the legal knowledge to back it up.

So, Jon, thanks for joining us.

Jon Praed: Thank you for having me Adrian.

Adrian Bye: You maybe want to just get us started and tell us a little bit about who you are, where you grew up and what you want to be when you're a big boy.

Jon Praed: Sure. I'm a Midwestern boy, born and raised in Indianapolis, Indiana, and went to college at Northwestern with a major in political science and then graduated from Yale Law.

I've been out of law school about 20 years and over that time, I have worn a number of hats. I've largely been mostly in private practice as a lawyer with Latham & Watkins in both California and Washington, DC but also right out of law school, I've clerked for some judges in Indiana – a district court judge, John Tinder who's recently been elevated to the Seventh Circuit and then the Indiana Supreme Court Chief Justice, Randy Shepard. I also spent two years working on Capitol Hill on the house side as chief council to a house subcommittee dealing with regulatory affairs. I've been doing this sort of cyber litigation work for about the past 10 years. I got into it when this small internet problem came about, known as spam back when AOL and other ISPs were first starting to recognise that there was this huge wave of cyber crime that was starting to come their way, and got engaged at that time, trying to really help these ISPs figure out how does one deal with this problem, and really create the legal mechanisms, enforcement mechanisms and political structures that you need to deal with the problem, and watch it over the past 10 years morph into the problem that it is today and really watch it continue to morph because I don't think we're yet at the conclusion of that.

That's my background in a nutshell. It's been an interesting ride.

Adrian Bye: Where do you live now?

Jon Praed: I live in Washington, DC suburb Arlington, Virginia.

Adrian Bye: Okay, because I looked at your site and you go back between the west coast and east coast. So you are based out in DC now?

Jon Praed: Yes, I'm based in DC now.

Adrian Bye: Right, okay.

I'm interested just first on the legal side. My brother's actually an attorney with Wilson Sonsini and he's doing in-house council work with Google on antitrust. You've taken a very different route to get where you've gotten. You didn't go into one of the big-name law firms. Is there a reason why?

Jon Praed: I started out there. I started out with Latham & Watkins after my clerkships, doing general litigation and so I think I've got that experience under my belt. I know how big law firms work and I know the value that they add. But I left Latham & Watkins to start Internet Law Group about eight years ago largely because it became obvious to me that the type of work that we were doing at the time is not the sort of work that big law firms really can do well. It requires a tremendous amount of expertise, and a team of people that really understand the problem and know how to streamline the work. A lot of our work is strategic in nature. It's not tactical. We represent multiple clients in identifying serial fraudsters and so the work that we do is really leveraged of learning how to acquire information on bad guys and make it available across a large client-base. That sort of work in our experience is best done with a small team of investigators and lawyers that you really can't put together in a big law firm. You're too isolated generally and big law firms stay big because they are good at weaving all of their practice groups into a cohesive whole. I think you find in big law firms if a practice group gets isolated and self-supporting, it leaves because it realises it doesn't need the things that a big law firm provides for it. So they generally will spin off into their own firm. I think that's inevitably what has happened with us.

internet
LAW GROUP

Adrian Bye: That's interesting. So the dynamic there is that you're basically a mile deep and an inch wide, and the big law firms are an inch deep and a mile wide. I guess that's an exaggeration but.

Jon Praed: Sure. Exactly right. I think while they certainly have their areas of expertise, part of their strength comes from their ability to handle a broad swath of problems that a corporate entity may have. Our expertise is really our ability to drill down and do things in somewhat in an innovative way as I hope we get into in talking about some of our business models. I don't know of other law firms in the country, big or small that are really approaching the problem of cyber crime in the way we're approaching it.

Adrian Bye: You want to just take it away and tell us a little bit about what it is that your firm does?

Jon Praed: Sure. As I said in a nutshell, we look for ways to bring strategic actions against cyber criminals. You've got to start with a good understanding of the problem that we're attacking. Cyber crime over the past 10 years has really transformed from petty crime and largely Americans who were kind of geeks gone bad. It has transformed from that sort of solitary criminal enterprise into an extremely sophisticated, extremely international criminal network. So the bad guys we are chasing are extremely talented, and are going to great lengths to hide their activity and to take advantage of the inefficiencies that arise from international boundaries. They're moving their physical bodies to places that are difficult for us in the west to touch and extradite from, they're moving their money to places that are difficult for us to freeze, and they're moving their computers and their connectivity to places that are difficult for us to touch as well. Because of that, you're seeing a convergence, I think, in the bad guy space between economic cyber criminals, terrorists and even nation state acts of warfare.

Adrian Bye: You think it's going to that sort of level?

Jon Praed: Without a doubt. Without a doubt, the bad guys – anyone that is on the internet doing something, trying to avoid identification and make money through illegal means has to jump through a number of hoops or they have to put on a number of masks to hide themselves. Their ability to do that is limited by the places that they turn to – the enablers, if you will, that they depend upon to give them the connectivity and the things that they need to do their business.

So our practice really specialises in first, understanding at a deep level the essence of how these cyber enterprises operate and then knowing what are their Achilles Heels because ultimately, we don't have to necessarily stop the entire enterprise. We have to insert a monkey wrench at some point in their criminal assembly line to stop the assembly line. If they can't process the criminal activity to its completion, they can't make money or do whatever it is they're trying to do.

Adrian Bye: How did you get into this in the first place? You obviously didn't study this in school.

Jon Praed: Yes. No, I was doing punch cards in college in school to give you an idea of the state of computers back when I was in school. I got into it really from private practice. Some ISPs reached out to Latham when I was there to take on this newfangled problem called spam which no one really at the time understood how big it would become and really what sort of a precursor it would be into the entire world of cyber crime. I got assigned to the case really out of serendipity but quickly fell in love with it and, I think, came up with some innovative ways to service the client, ways that involved really marrying our ability to crunch a tremendous amount of data with our ability to bring legal services to bear on the problem. By marrying those two skill sets, we've really been able to make head roads into figuring out how does one get at identity behind the cyber criminal problem and put a stop to it. So I had gotten into it doing that spam work but since then it's morphed into representing far more than just ISPs. We represent financial institutions, drug companies – really any sort of corporate victim of substantial, systemic, serial cyber fraud whether it's a counterfeiting problem with drug companies, phishers going after bank customers, or mail companies that it's either mail systems expand fivefold because they're trying to deal with inbound spam problems or even outbound spam problems.

Adrian Bye: How big is your practice?

Jon Praed: In terms of what?

Adrian Bye: Attorneys or people.

Jon Praed: Well, I don't talk much about our size. We're a small firm. We've got less than 20 folk doing the work but we've got some technology sitting behind what we do. Our technology allows us to grab what we need from webpages, e-mails and other indicia of cyber crime to capture the evidence in real time that we need to get at identity.

Adrian Bye: I would suggest that, that's a sign of doing things right. The best internet organisations that I see now are the ones that have small teams at 30 or less people and more often 20.

Jon Praed: I think that's exactly right. I love the idea and it's been fun to work in a small firm environment because I'm enamoured with the skunk work's mentality of stop worrying about what your job description is and start thinking about how to solve the problem.

Adrian Bye: Yes, very much so.

Jon Praed: We focus on that question…

Adrian Bye: That's also spoken like an entrepreneur. Employees don't always like it that much.

Jon Praed: Yes. Some do. I think you either thrive in that environment or you don't.

Adrian Bye: Yes, sure.

Jon Praed: It can give you a lot of freedom of thought and opportunity to be creative but you've got to have some creativity to bring to the table.

Adrian Bye: For sure.

You won some big cases. Have you gone after guys like Sanford Wallace and some of these others? I mean where did this start out and what are some of the big cases that you've been involved with in the past?

Jon Praed: Sure. Well, we've had a number of cases that have been litigated and produced some published opinions that have had some impact in the world of cyber crime. A couple that I can mention – we had a published decision in a case we brought for America Online against an adult website called Cyber Entertainment Network that was brought in 1999. The decision was published in 2001 that really established – AOL had sued Cyber Entertainment Network for hiring affiliate advertisers. It's the affiliate advertising model that your listeners are probably well familiar with. But in really suing Cyber Entertainment based on the principle of negligent enablement, and negligent hiring and retention that they had retained affiliates that it either knew or should have known were engaged in spam to advertise their websites and that on that basis, they could be held liable. So we used some fairly aggressive technology there to grab the data we needed and establish that a large volume of the adult content spam that AOL was seeing at the time was attributable to spammers advertising one of a handful of adult websites controlled by Cyber Entertainment Network, and that the individuals behind those spam messages could be identified through their affiliate codes and that some of the affiliates were cycling through serial affiliate codes. When they would be identified publicly – an affiliate code would get identified publicly – they simply flip to a new affiliate code and continue the process. Sort of wash, rinse and repeat.

Adrian Bye: So you were able to prove that because that's actually obviously one of the frustrations of the affiliate marketing community as there's been a perception for quite awhile that affiliate marketing isn't legitimate. I don't know. I guess that's slowly starting to change. I'm in the camp that I know profoundly that it's a vital part of internet commerce and has to be. I mean there're even companies like Amazon that have been using it for a very long time. It's been frustrating hearing guys coming out and saying that affiliate marketing is bad, and you shouldn't do it just because it's filled with spam. I've had conversations with Spamhaus on that sort of stuff. Where do you stand on that stuff?

Jon Praed: I think you and I agree. A properly-run affiliate program can be extremely powerful but the key is it has to be run effectively. You have to recognise there are opportunities for abuse and that you are effectively outsourcing your advertising. You have to do so with clear standards in mind and you have to enforce those standards. It starts with the simple requirement to have identity. You've got to know who your affiliates are, communicate to them what the rules are, investigate reports of abuse and effectively adjudicate those reports even if it's just an internal adjudication. So you've got to tell your affiliates that they will be terminated with prejudice if they don't follow the rules.

Adrian Bye: Is there any kind of list out there of like here's the standards of what you should follow for affiliates?

Jon Praed: I am glad you asked. The public injunction that was entered in the AOL versus CEN case, I think, remains the best model I've ever seen on how an affiliate program needs to be run. That injunction which is public…I think you can get to it from our website…lays out the rules that Cyber Entertainment agreed to follow in the course of the outcome of that litigation and it lays out those simple standards – get identity from affiliates, establish rules, have a mechanism to receive complaints from the public, investigate those complaints, report back to the public on the outcome of the investigation and terminate when necessary. If you do those things, you will have a clean affiliate program. If you don't do those things…

Adrian Bye: But they still have to do a lot of that stuff anyway because one of the big issues they have is affiliate fraud where guys are signing up from weird countries and then they're getting commissions on things like gift cards like they might spend $1 on a gift card and then get $20 back. That's almost wiped out a bunch of companies. I think it's getting under control now but they have to have a lot of control now anyway just to manage stuff so obviously, this should be happening anyway to manage spam.

Jon Praed: Right and it's just sort of an extension of the mindset. The affiliate operators for a long time have focused on affiliate fraud that hurts their bottom-line but they weren't focusing on their long-term bottom-line.

Adrian Bye: Right.

Jon Praed: That's something that I think too many people operating on the internet aren't thinking about – their long-term risk of liability to third parties who may be hurt by internet conduct that they are enabling. I think that's really the wave that we're in today is of trying to help good companies throughout the world understand the myriad ways in which they are enabling in some way or another serious cyber crime.

Adrian Bye: The problems is…because I've been on both sides of this and so I think we are very much in agreement but…the side that I've seen is that we get told that affiliate marketing is bad and it's just for spammers anyway so you just shouldn't do affiliate marketing. That's wrong. I think what you're saying is the correct approach but when you've got these guys saying that affiliate marketing is wrong when we know and just know. It's like a political or religious conviction. I know it is an absolute integral model of the internet that it's hard to take the rest of what they say seriously.

Jon Praed: Yes, I think that's right. I think a lot of people view affiliate marketing as simply a sanitised word for criminal marketing and it's not.

Adrian Bye: Yes.

Jon Praed: We need to break that connection and I think you do that by focusing on the characteristics of the affiliate marketing program. If you have proper characteristics, lawful characteristics – it can be quite powerful, profitable and useful for you.

Adrian Bye: Are you seeing people's mindset change on that sort of stuff?

Jon Praed: Yes, I think so. I think particularly after CAN-SPAM was enacted, you had a lot of legitimate marketers who were looking for a way to distinguish themselves from illegitimate marketers and they viewed CAN-SPAM as that sort of signal opportunity that if we do it this way, we're CAN-SPAM compliant and our marketing methods will be accepted as legitimate. I think CAN-SPAM has helped clear the middle of the room of both legitimate and illegitimate marketers. It's required them to go to one side or the other and most legitimate marketers today, I think, are doing a fantastic job of servicing their clients and getting ads in front of eyeballs that really want to see them.

Adrian Bye: Fair enough. I'm really heartened to hear you saying this. It's really good to hear.

Jon Praed: Before we talked, I sort of eluded to a point that I think complicates all of this. To me, cyber crime is a tremendous problem. Most people though conflate it with the overall problem of how do good actors within the internet compete with each other appropriately, and how do we resolve disputes between and among them. I try to make the analogy that no one has yet put their finger on exactly what cyber crime is like. This is a brand-new thing yet it's not. We have dealt with this before and the analogy that I've come up with that I think really works and captures this problem is the analogy of a riot in a bazaar. It is the equivalent of a cyber riot in a crowded marketplace that is full of lots of other people – innocent victims, both who are merchants and consumers. Cyber criminals are acting like both merchants and consumers at various times, running through this bazaar and trying to engage in their criminal enterprise. So our ability to fight those cyber criminals is complicated by the fact that the battle space is inhabited by lots of innocents that are indistinguishable from the bad guys. So part of our fight is to try to remove those innocents from the battle space and also remove battles between them because their battles are uniquely different from the ones were fighting against cyber criminals. Where you have a commercial dispute between a merchant and a consumer over whether the consumer really agreed to the terms of service, for example – you know who the consumer was. Consumer is not usually trying to hide their identity in the first instance. So many of these commercial disputes that take place on the internet take place between two…I call them…white hats where neither of them is trying to hide their identity, they're all in business for the long term, they're trying to build value around a brand that they willingly advertise and pay good money to advertise, and they are engaged in business in the same space that the bad guys are in that we're trying to catch who are not investing in any brand, aren't using their real names ever, and are doing everything they can to hide and simply find some way to exploit the system to make money. So a lot of the debate that I hear out there, to me, is interesting at one level but it's also a debate I don't engage in because I'm trying to make a practice where we get corporate victims to band together to identify and stop serious, serial cyber crime. If we can do that, the space in the commercial market will change substantially. The cost of doing business will be reduced substantially that these other sort of grey disputes where both sides have at some point a legitimate position are going to be clarified and in many ways simplified.

Adrian Bye: When do you see that happening?

Jon Praed: Good question.

Adrian Bye: I mean every year, it does get better. It does get clearer.

Jon Praed: I think it does. I think it is a slow process. I talk about the maturing of the cyber crime lifecycle. I think we are still only in the teen years of the maturation process for cyber crime and by that I mean we are not yet close to a static state where cyber criminals and their systems have developed as far as they can develop. Until that happens, we are going to continue to chase them, and they're simply going to retreat back to darker and darker places in the world that make it harder for us to get to them. I think we're going to see a dichotomy in the next 10 years or so – a division within the internet government space where a couple of major countries whether it's China leaving ICANN or the United States leaving ICANN – I think you're going to see a division between nation states that emerges that finds cyber criminals on one side of the divide and law-abiding citizens on the other.

Adrian Bye: When you talk about cyber criminals, in general the area of the bad guys, you're not seeing them in the US anymore. You're seeing them all in countries like China or in places like that.

Jon Praed: That's the thing. No, we're not. We're still seeing many of them still physically living in the United States. That's why I say we're not yet past the teen years in this maturation process because we have seen some cyber criminals who are Americans who have physically left the United States but they have not given up their US citizenship and in a post-9/11 world, they have some hard decisions to make. This is all of the development of the law. If you're an American citizen, wherever you live in the world, you're still subject to certain de minimis laws of the United States and not many people know this but there is a law that allows private civilians – civilian litigants to ask a judge to order an American anywhere in the world to return to the United States to be deposed. It's not used very often but it is available and I anticipate that it will be used more and more in the cyber arena as US citizens flee the United States but don't give up their citizenship because that's a hard thing to do.

Adrian Bye: The people that are doing this from the US – are these the people that we see on the ROKSO list? I mean who are they?

Jon Praed: They are or their aliases are on the ROKSO list. I think that the ROKSO list is a pretty good indicia of who the big actors are.

Adrian Bye: So you do feel that ROKSO is accurate?

Jon Praed: Yes, it's accurate in terms of what one can know about who these actors are without the power of subpoena. ROKSO listed Jeremy Jaynes as Gaven Stubberfield years back at number eight on the ROKSO list and I have no reason to question their ranking that Gaven Stubberfield was number eight. But he wasn't Gaven Stubberfield. His real name was Jeremy Jaynes and you could only figure that out through a subpoena which requires you to have legal process. So there are certain internet data points about bad guys that Spamhaus and others may collect that serve as good placeholders for identity but they're not pure identity.

To me, the battle we're fighting is to try to force the cyber crime enterprise to mature more quickly to get to that static state that I've described so that we can then bring greater force to bear against the bad guys wherever we find them ultimately residing and to do that, we need to much more aggressively use, in my view, the civil litigation process. We're spending billions of dollars collectively on technology to filter, block and in one way or another deny access to internet data points that in one way or another we've decided should be blacklisted, whether it's domain names, IP addresses, e-mail addresses – what have you. But none of those data points are inherently tied to the human beings engaged in this conduct. So we are constantly playing a game of cat-and-mouse on the technology side and we are starting to have government enforcers engage in the long, drawn-out battle to identify and arrest these bad guys. But anyone that's played that game knows that's an extremely long, slow, cumbersome process and there is a huge middle ground that is largely unoccupied. That's where our firm stands and that is finding a way to use the civil litigation process to accelerate the transformation from internet identity data points to real identity data points and then once you have identity, strategically identify something that can be done to those human beings, whether it's suing them civilly, making a referral to government authorities or reinforcing technical filters to keep those people from getting access to the internet tools and services they need to continue.

Adrian Bye: Looking at the ROKSO list, there's a guy like Alan Ralsky. He's been known about for a very long time.

Jon Praed: Yes.

Adrian Bye: He's living somewhere in Michigan. I mean what's the issue with stopping him from doing what he's doing?

Jon Praed: Well, we were actually the first people to identify Ralsky. I caught Al Ralsky for Verizon Online back in 2001 and we got a judgment against him in 2002. That's one of the cases that really changed the space because Ralsky argued at the time. We sued him in Virginia. He was working out of Michigan and we sued him in Virginia, arguing that someone who sends out bulk e-mail without regard to where it's going to land can be sued wherever their spam lands. He tried to argue that he could only be sued in Michigan and he lost that case. We won a summary judgment victory that was quite important in establishing essentially spammers can be sued wherever their spam causes injury. But we caught him in 2001. The federal government – the FBI raided his house, I believe, about a year ago and finally busted him allegedly for engaging in pump-and-dump schemes spam advertising Chinese stocks.

Adrian Bye: Chinese stocks?

Jon Praed: Yes, Chinese stocks. He had a large enterprise of people that were helping him, some in China but most in the United States. So he can get caught but if we wait for government law enforcement to catch them, you're going to wait years longer than you otherwise need to wait then it would take if we can engage in self-help through private actors.

Adrian Bye: So you basically get a bunch of big companies to bankroll you to go after guys like him to stop him?

Jon Praed: In essence, yes. In essence, that's what they're doing by paying taxes to hire government law enforcement. The trouble is government law enforcement has resource constraints, political constraints and even legal constraints. The criminal process is intended to be an inefficient process because we don't want to make it easy for citizens to be arrested and accused of crimes, properly so. But we also have a civil litigation process that exists for good reasons as well to allow private actors who are hurt to seek redress for those injuries.

Adrian Bye: Right. No, I get it.

I know that your focus is on the black end of the spectrum. I do want to ask you more questions on the grey area because this is something that's relevant to a lot of this audience, if you don't mind.

Jon Praed: Not a bit.

Adrian Bye: One of the areas that's interesting to me is CAN-SPAM. First out, what is your opinion of CAN-SPAM law?

Jon Praed: From 100,000 ft, it's an arrow that's nice to have in your quiver of weapons but it is not a silver bullet and I think anyone that thought it would be a silver bullet was naïve.

Adrian Bye: For me, the thing I don't understand about CAN-SPAM is that it creates a very big loophole to easily walk through that's totally legal and just hasn't been sorted out yet. I don't understand why so I'm very happy to have you here today where I can now ask you this as my big question. When people sign up to my CEO list, I can put terms and conditions, privacy policy, and all that sort of stuff on the site. My privacy policy could say that I choose to make all of my e-mail addresses available to Chinese Viagra spammers and I'll also give them to whoever else I choose to give them to. If I'm really bad, I know I can put a checkbox on my site and say, "I agree to the terms and conditions of signing up to the MeetInnovators private CEO list." They've then opted in to whatever is written in my privacy policy and I can put whatever I want in there and that can include reselling my list to as many people as I want to resell it to, give it to or whatever I want to do with it. I don't understand why that is allowed. Can you maybe help me understand that?

Jon Praed: Why you're allowed to essentially resell your list?

Adrian Bye: Why I'm allowed to bury the terms of reselling my list in things like terms and conditions?

Jon Praed: Sure.

Adrian Bye: In this point, even you, I imagine, don't read the terms and conditions of every site you opt into and maybe you do. But Grandma Jean in Nebraska is not and she's never going to read that sort of stuff. I don't know why it's set up so that she would even have to consider reading terms and conditions or something like this.

Jon Praed: Right. The reality is most people won't and so you're going to do what you want with that e-mail address. But if you have made disclosures, you can and should be held to the limits of those disclosures. If it turns out that you're doing something with those e-mail addresses that the owner of the address doesn't want to have happen, they should have the opportunity to opt out.

I think it's very hard for government to get into the business of defining certainly in a federal statute that 435 congressmen and 100 senators have to vote on that spells out exactly what fair notice means in…

Adrian Bye: But to me, it can be solved simply. I mean let me give you an example. What if there was a condition of opting into a bad guy's list that says, "I agree to have my e-mail address resold 200 times," so as soon as they opt in, it's resold 200 times. So they can opt out but they're going to now have to opt out 200 times. I've heard from the other standpoint guys who'll say, "When you get those fresh e-mail addresses, you've got to mail them quicker and more than everyone else because you've got to mail them before they go dead."

Jon Praed: Right. But ultimately, a lot of this debate is over consent. This is again one of the grey areas that people like to debate but it's not as interesting to me because I have had marketers argue to me that they had essentially a blood test and a spinal tap from the consumer that gave them consent to do what they're trying to do with the e-mail address. I have said to them, "The consumer changed his mind, the consumer has the absolute right to change their mind and you as a marketer can't do much about it." The best marketers are those who understand that the value they have is getting value in front of eyeballs that want to see what they're advertising. If there's a disagreement between a marketer and a consumer at some level, write the law however you want to write it, the consumer's going to win that fight because you're…

Adrian Bye: They're not though. Right now, the consumer's losing. The way I see it as a simple solution is let's say they're signing up for my domain, meetinnovators.com and as you sign up, it says clearly on the signup page, "Your e-mail will come from meetinnovators.com and that's your license to e-mail from that address," and that's it. You have a relationship then with that domain and that address, and that's where your e-mail comes from. If you want to go changing it then you can opt your list back in. To me, that's a solution. I'm so torn on this and I don't understand why it happens in another way. It seems like at this point, they should be well-enough understood.

Jon Praed: Yes, I think ultimately though, innovative marketers and effective marketers are going to develop systems that intuitively monitor and react to consumer preferences. To say that someone can strong-arm a consumer or has a right to strong-arm a consumer to me is a losing argument. It may take awhile for that sort of business to die but it's inevitably going to die.

Adrian Bye: Yes, I mean it's still there today and it's billions of dollars in business.

Jon Praed: Sure, but I think as marketing gets more and more targeted, and as consumers get more and more aware of what their rights are, and where they can go on the internet to see the things that they care about and express their preferences, and they see marketers reacting to their preferences – you're going to see them gravitating to those sorts of mechanisms.

Adrian Bye: But see, here's the point. To get opt ins like this, let's say I can support putting on my website, "Put your e-mail address in here and you'll get $1,000 in cash." If I can buy more media than anybody else by having the strongest offer then I'm going to be able to collect more e-mail addresses from these people who don't read the terms and conditions.

Jon Praed: Sure.

Adrian Bye: Case in point a few years ago. I'm sure you're very familiar with all of the spyware stuff. Those guys doing illegal spyware installs were able to pay the most for traffic because they were able to monetise the most effectively because they drove everyone the most crazy.

Jon Praed: But they still in the end have to have something to sell to those eyeballs.

Adrian Bye: Popups. There're popups on your computer. That stuff has obviously gone away but there's still a lot of this like the race to the bottom. The guy who can pay the most for traffic, monetise his list better and do the most aggressive stuff for the list is able to get the biggest list.

Jon Praed: Yes.

Adrian Bye: It becomes very hard to compete with.

I don't know. If we're going in an area outside your expertise, tell me.

I see this as kind of a defining point in e-mail for me.

Jon Praed: I would agree with that but I think that in the end, the long-term play is going to be the empowerment of the consumer and marketers are going to develop techniques that more accurately capture consumer preference. I think you already are seeing illegitimate marketers. Spam has always in my view been illegal regardless of what the law says. It's socially improper and things that are socially improper have been illegal for a long time. So even before CAN-SPAM came along, spam was illegal under state law and all sorts of other laws. But spam is really now married to illegal product because spammers have nothing left to advertise and people selling illegal product or product that is regulated in some ways…say, counterfeit drugs, for example…are naturally attracted to each other because they need each other. Spammers need something to advertise.

Adrian Bye: So it's a cesspool that was a lot larger, and is gradually shrinking and shrinking each year, is that accurate?

Jon Praed: I think, yes. I don't know that the pool is shrinking but it is starting to segregate itself from the pool of legitimate marketers and legitimate manufacturers of goods and services who are gravitating towards legitimate marketers. Yes, there maybe things like click-through ads and other types of advertising mechanisms that are still in the middle bollixing up this dichotomy between lawful and unlawful but I think we're starting to see the endgame where those middle actors are having to move left or right – to the lawful side or to the unlawful side.

Adrian Bye: I think there's a lot further to go. I guess what you said, maybe it is going to take another 10 years – I guess I'd agree with that.

Another point I'm interested to ask your opinion on is I tag my e-mail addresses so when I sign up for different sites, I tag them with the domain so that I can see where the different mail is coming from.

Jon Praed: Yes.

Adrian Bye: I signed up for a site called Bid Brain and another called Template Monster, and in both cases, I've noticed various types of porn since come into those addresses including in the case of Template Monster, bestiality porn.

Jon Praed: Yes.

Adrian Bye: I'm pretty surprised by that. What actually is happening behind the scenes? I mean this is just Template Monster. I bought a template from there for a website.

Jon Praed: Yes. Well, I don't want to touch on any particular website that you may be mentioning but the problem overall is one that's really an old model. There are lots of websites that are out there selling things that are really being used for ulterior purposes – people who are looking to try to get e-mail addresses or they may be victims themselves of data breaches where their e-mail databases are being stolen.

Adrian Bye: In these cases, these are both legitimate fairly popular companies and so certainly there's no bad stuff intentionally going on. It must have been some kind of a breach. I was really shocked to see this from two of these companies. They look like they've got their act together.

Jon Praed: I think that your system of tagging e-mail addresses provides you a view into those sorts of problems that you're going to see more and more people doing, and even companies commercialising in a way. You already see throw-away credit cards. You've got throw-away e-mail addresses. The ability of consumers to personalise their identity in ways that give them a great view into how their data is being used – there's a tremendous amount of value in that, getting that into the hands of consumers and then collectivising what we all can know about the things that people are doing with this data as a result. So it'd be interesting to know what other people's experiences that those websites or other websites are like so you can really see patterns and trends. If there was a data breach, you can determine down to the day or the minute when the data breach took place based on when various e-mail addresses were posted there.

Adrian Bye: Is there a place where a guy like you gets reports on that sort of stuff that we can send it to? I know there's obviously the FTC address and there's been SpamCop but are there better places now?

Jon Praed: Sure, there are a number of reporting websites that take in that data. We have one that we operate called reportphish.org where we receive reports primarily about phish but also about spam and other types of fraudulent acts that can be reported to us. You can send it to report@reportphish.org or you can register at that website and get a unique e-mail address that can then use to forward your particular reports to us so that they are tagged as coming from each registered user.

Adrian Bye: Do you get a lot of reports through a site like that?

Jon Praed: We do.

Adrian Bye: I mean so because the stuff like that – it's just general phishing stuff. I mean there's a lot of that out there. Actually, why don't you tell us a little bit about phishing and what's going on?

Jon Praed: Well, the phishing problem, I think, is really integrated within the overall cyber crime problem. We're chasing some cyber criminals today who are engaged in phishing, cashing out of stolen credit cards and at the same time are merchants that are part of a nationwide and international credit card system. They're authorised to take credit cards over the internet. They're successfully processing cards from consumers, selling them product and getting credit cards.

Adrian Bye: So the things like that – wouldn't that be trivially easy for you guys to go after their merchant account and stop them?

Jon Praed: It's not trivial but certainly using our process, I think it's a viable mechanism to putting a stop to it. But again, the path that connects their phishing activities with their merchant credit card activities is an extremely long path, and it takes a tremendous amount of data and sophistication to connect the dots.

Adrian Bye: I used to think phishing was just for idiots. Probably a year after it really started happening, I got caught by a phishing attack in PayPal. I logged in and entered in all my PayPal info. I did the same on an Amazon site too.

Jon Praed: Right.

Adrian Bye: It was early in the morning. I got up and I was sort of checking my e-mail. It said, "Your PayPal account is going to be shut down," so I log in and enter it all in. Thirty seconds later, I'm like my god, what have I just done?

Jon Praed: Right and that's the problem with the block-it, filter-it strategy that we've largely adopted today. The bad guys only have to get through one time in order to win and so if you block them 99 times, they'll do it 100 times and if you raise your accuracy to 99.9%, they just have to get to 1,000. So you're in a constant arms race in the technology space that inevitably we're going to lose. That's why you've got to do something with those incidences that are a technological loss to us. You've got to take those and chase them somehow, and have some offence to the defence.

Adrian Bye: Yes.

Jon Praed: Right now, we as a society are woefully inadequate in playing offence in this game.

Adrian Bye: I think it's getting a lot better. I mean I'm using Google Apps for my e-mail and I'm pretty impressed with the job they do on filtering. I think they do a pretty awesome job.

Jon Praed: Yes.

Adrian Bye: I used to have to personally take all my tagged e-mail addresses and filter them all to my spam folder.

Jon Praed: Yes.

Adrian Bye: I found now that very little spam gets into my inbox. They just handle it. I think things are improving a lot.

We're actually on the edge of our time. I still have a bunch more stuff I would be interested to ask you about including some of your things – what you're doing with companies that have brands that are getting those abused. But if you're out of time then let me know.

Jon Praed: No, I'm fine. I've got a block still open so if you want to keep going, it's fine with me.

Adrian Bye: Okay.

On that point of filtering, what are your viewpoints? I mean obviously, I'm happy with Google Apps. I'm probably using one of the better systems out there. Are you involved in that side on the sort of stuff that people like Anne Mitchell are doing?

Jon Praed: I'm a little bit. I think the technology is always going to play an important part. My point has always been I think that we have been too reliant for too long on the technology without recognising how legal process can reinforce what technology is capable of doing. I think technology in a way is like trying to nail Jell-O to the wall. We may be able to fix one component but three new exploits open up constantly. Despite the fact that your experience seems to be good with respect to inbound spam, the overall spam volume on the internet is still growing. It's at 90% and growing, and I don't see that trend reversing itself for a long time. It goes well beyond spam. The number of new viruses out there is growing constantly. The number of exploits, keystroke loggers and whatnot – those problems are simply getting larger and larger. I think that criminal enterprise that's behind it is getting more and more sophisticated and adept at finding a way to monetise the data that they're able to capture through these sorts of exploits.

Adrian Bye: You mentioned they're moving offshore and obviously you know that I live in the Dominican Republic. You said that there are guys that are down here that are in Panama or in Dominica. What's going on? What are these guys doing? I mean I'm down here and obviously that means people look about and say, "My god, what's he doing down there?" I don't know any of those guys and I don't even know where they would be. Where are they setting up and what are they doing?

Jon Praed: Yes. Well, some of them, I think, are going just where they want to go but many of the ones that are the most sophisticated are moving their persons to places where they are physically insulated from law enforcement. They're looking for places where they can pay off local authorities to provide them protection from criminal enforcers and from extradition.

Adrian Bye: That definitely works in this country.

Jon Praed: Yes, but I think again, many of them are…

Adrian Bye: I think this is one of the top 10 most corrupt countries in the world.

Jon Praed: That's why I say there's a convergence between cyber crime, cyber terrorism and even acts of cyber warfare. You're going to see all those types of bad guys gravitating. Their bodies, their money, their equipment are all going to end up in the same general places.

Adrian Bye: So it's a little bit like the stuff we see today around money laundering and then there's all the KYC – Know Your Client and that sort of stuff to keep the banking system clean. But there's also a king of a firewall between mainstream big countries and then some of the more shady countries. Is that what we're going to see with spam as well?

Jon Praed: You're already seeing it. Those who are engaged in it – a lot of our work comes down to tying identity to these internet data points and then marrying that up against pre-existing laws that already exist, that make these cyber crimes criminal in dozens of ways. They're all violating tax laws. They're breaking money laundering laws. They're breaking all sorts of laws on importation of goods. It's not hard to find something that they're doing that's illegal. The trick is knowing who they are.

Adrian Bye: I can tell you from the standpoint of living down here, it's made my banking a real big hassle. I'm not doing anything wrong. The stuff that you have to go through – the KYC regulations are a real pain.

Jon Praed: Yes.

Adrian Bye: I mean that's good. That really will create a firewall that's going to stop them.

Jon Praed: Exactly at 100,000 ft, what we're trying to do as a world view is create borders, whether they're technical borders, physical borders or what have you that allow us an opportunity to inspect, whether we're inspecting internet cyber packets or we're inspecting transactions – loads of money.

Adrian Bye: So all you bad guys, you go off there and live in…hopefully not the Dominican Republic but they can go to…Panama, for example. So all the bad guys can go there and so then you can then inspect more closely the traffic from Panama.

Jon Praed: Right, you can tighten up the border and you can ultimately just cut off the border completely. That's why I think we're going to be facing more frequently over the next decade a real blacklist where certain types of traffic, whether it's flow of humans, flow of money or flow of information – there're going to be borders that simply aren't porous. They don't let information through.

Adrian Bye: Which are the countries you see that happening with?

Jon Praed: Well, I think you've got a lot of bad guys in Eastern Europe and Russia. I see South America and I see Asia developing as real havens in some ways or another, whether it be computer resources, money laundering or physical protection.

Adrian Bye: I've got to tell you. I mean I've travelled a lot and lived in a lot of different countries. Let's say that the Dominican Republic did get grouped into that. A guy like me that lives here – I have hundreds of friends locally that are normal, good people and the concept that their internet traffic would just be blocked is almost a little bit hard to believe. Do you think it will come to that standpoint where the US says, "Okay, Dominican Republic, we are shutting you off the internet until you make sure that your country is completely cleaned up and as soon as you're cleaned up then we'll let you back on."

Jon Praed: Sure.

Adrian Bye: Is it that kind of thing that will happen?

Jon Praed: The binary decision of turning the valve completely off will happen at the margin but in-between all open and all closed, you have an entire spectrum of controls that you can put in place. A lot of that is designed to simply put on those people who are best-positioned to fix the problem, the cost and obligation to fix the problem. Yes, citizens of a country have an obligation and it's interesting that we're having this conversation on Election Day in the United States. I think the post-9/11 world makes everyone as a consumer and as a citizen sit up and realise wait a minute, I can't wait for my government to fix all of the problems out there. We as individuals have an obligation and a duty, and the right and the ability to step up and fix these problems.

Adrian Bye: This comes down as someone like ICANN gets together and says, "Okay, Dominican Republic, there are 9 million people there and you might have 10 guys that are bad but we're shutting all of you off the internet until this is fixed. So therefore if the government is so corrupt that it can't handle it, it's going to kind of, not force the citizenry but it's going to motivate them to push government to clean itself up to fix that. Is that the direction you see it taking?

Jon Praed: Sure and I don't know that it will just be a binary decision out of the cold to either fix it immediately or go dark but there will be those pressures of isolating the problem and putting on the people who control those access points, responsibility to clean up their act. It's just like the cleaning up the affiliate model, right? We couldn't go after Cyber Entertainment Network until we knew that the websites ultimately being advertised were all in one way or another controlled by Cyber Entertainment Network. Once you make that connection, it's relatively easy to find the ultimate owner and say, "You've got a problem. You've got to fix it."

Adrian Bye: I get it. It's just it's hard to hear it because these are so many good people here and some of them are just in poverty. This is the kind of stuff that pushes them down even further but I can see why you do it too.

Jon Praed: You can view it though as pushing them down but you can also view it in an alternative way as empowering them because it does. It gives them the power to control their own destiny and the obligation to do it. I think what you really have to look for are mechanisms that get caught in a race to the bottom, as you said earlier.

Adrian Bye: Right.

Jon Praed: What we have to avoid are creating systemic mechanisms that encourage and reward races to the bottom, and I'm a little afraid that the internet as a whole, given the power of anonymity and the ability to do things in an automated fashion, creates at some level a race to the bottom.

Adrian Bye: So it does.

Jon Praed: You have for example goods manufacturers and drug manufacturers who are for the first time really seeing counterfeiters who before had to sell their goods from the back of a truck now have access to the world as a whole, and have access through spam and other types of advertising to billions of eyeballs throughout the world. So finding a way to address that problem, recognising the inefficiencies in our legal enforcement process is a very hard thing and I'm a little afraid that we do have a race to the bottom where good companies like that, that are dependent on legal mechanisms to give them the ability to invest hundreds of millions of dollars to develop a new drug – if they can't recoup that cost, we're not going to get new drugs developed. Right now, they are being challenged by bad guys who are selling counterfeits, knockoffs or generics made out of countries that don't recognise patent rights.

Adrian Bye: Yes, it's the same issue.

Jon Praed: So we've got to find a way to, I think, jumpstart to recognise those systemic races to the bottom and put in some sort of stopgap measure that prevents that from happening.

Adrian Bye: As much as this sucks, I think regulation is really the only way to get a lot of this in properly because where you're describing in the case of drug companies and knockoffs in non-patent-respecting countries for a lot of our stuff, it's, "Hey, I can't buy as much media as this other guy because he's doing things that are 1,000 times more aggressive than I am" and they're currently legal because there're no laws passed against them.

Jon Praed: Right.

Adrian Bye: So do I do those things to so that I can compete with him on media or do I not and then have a business that's 1/1,000 of the other guy?

Jon Praed: I don't think in the end you're going to solve the problem by informing those sorts of individual choices. What you have to do if you have a systemic problem that is the race to the bottom, you have to find other mechanisms that almost screw the other way. They corkscrew the other way that are races to the top. You have to create jurisdictions that are defined by borders where the borders are defensible and you have to create those jurisdictions with rules that encourage races to the top.

For example, everyone knows that Delaware state law is favourable to corporations which is why most corporations of any substance incorporate there. Lot's of people talk about Delaware state law being a race to the top that of all the state laws out there, Delaware is at the top of the hierarchy because it provides the most stable, predictable, efficient legal process for companies and anyone trying to maximise profits is going to incorporate there.

We need that same sort of mentality to be brought into their internet systems and then defend those systems so that they can serve as a counterweight against these races to the bottom, segregate those jurisdictions that do suffer from races to the bottom, and isolate their problems within themselves so that they are incentivised to clean themselves up and ultimately have to in order to rejoin the rest of the world.

Adrian Bye: That's a fascinating idea. Where can I learn more about that? Who is someone that talks about that stuff, their book's on it or…

Jon Praed: There are a couple. A classmate of mine, Jack Goldsmith wrote a book called *Who Controls the Internet?* that I think provides a refreshing realistic perspective on how jurisdictions do retain power over the dirt that they control. It is refreshing to see that even the internet is subject to those sorts of real politic notions of power and control. I think there are also some books being written about the economics of cyber security and cyber relationships that will drive a lot of this because a lot of these systemic problems are going to be how can we monetise the value that's inherent in the internet. So understanding those systemic efforts to monetise the internet I think are going to be important to understand the problem. But you know, it's a psychology experiment. It's anthropology. It's economics. It's politics. It's law. That's why I think the internet is so fascinating for so many different types of people because it really does…

Adrian Bye: That concept of race to the top is one of the most profound ideas, I think, I've heard all year. That's something I've been struggling with for years. I'm going to get Jack's book and if there's any other resources on that, I'd love to know about them.

Jon Praed: I don't know of many others. There may be sort of a deficiency in the literature right now about that but certainly again, the internet may be new but the concept of building systems that generate a race to the top is not new. There's lots of literature on that in other fields of study.

Adrian Bye: What would be a field of study that successfully solved that problem?

Jon Praed: I think the development of state laws. I think there are lots of organisations that are looking to develop model state laws that integrate good concepts that encourage races to the top versus races to the bottom. The Association of Attorneys General or there are a number of legal organisations that try to develop model laws that various states can adopt, whether it's the UCC or electronic commerce laws – what have you.

Adrian Bye: Are there any others? So building state laws. Are there any others that have reflected that problem being solved?

Jon Praed: Well, I don't know about the ultimate solution. I think you're going to see it in the money laundering world. Probably in a lot of legal environments – patent protections. I think you'll see some literature that talks.

Adrian Bye: It's happening in the patent-protection areas, you mean?

Jon Praed: Well, yes. I think lots of people have talked historically about the value of patents and that it is really a right that developed countries more than undeveloped or developing countries recognise and respect because they have the assets to protect there. Countries like India have generally inferior patent protections because India doesn't have a lot of innovators and as a result, as India develops, innovators are going to flee India because they can't get the protection that they want, and as India.

Adrian Bye: So they need to be encouraged to build in this race to the top type system for patent protection which will encourage their entrepreneurs to stay in India and build the kind of companies that can help them grow.

Jon Praed: Exactly.

Adrian Bye: I'm going to really look into this. That's an amazing idea. Thank you for sharing that.

Jon Praed: My pleasure. I hope it resonates. A lot of this, the internet's not developed and these theories aren't developed.

Adrian Bye: No, because I've been struggling with this and there's been no direction to go in. You've just pointed the way and that clearly is the right answer. Who knows how to do it but at least that's the path.

Jon Praed: I think the key is to focus on precise things that we're doing. It's things like we have to have borders. I've been saying this to a lot of technology folks and asking them in the technology space, "Come up with a router or some piece of technology that can recognise physical geography and jurisdiction."

For example, let's give Grandma the ability to surf the internet but tell her browser that she only wants to go to places supported in the United States, places that she would physically travel to. Grandma doesn't want to go to Malaysia, she doesn't want to go to North Korea, she doesn't want to go to Russia – places that Grandma just has no desire to go to. Give her the ability to translate that physicality into her internet experience or her e-mail experience and give law enforcers the ability to say to bad guys, "You're crossing a border. You're now on my dirt and if you do something wrong, I get to do something to you." Create a carrot-and-stick mechanism that rewards good behaviour, and punishes and deters bad behaviour. If we can find a way to marry that sort of technology with jurisdictional borders, you're going to accelerate the ability of law enforcement whether it's civil or criminal to start throwing carrots and sticks out at the world and encourage this sort of race to the top because it can't be a race to the top until there are real carrots and sticks that work.

Adrian Bye: Yes. Exactly and those will come over time. Fascinating.

Jon Praed: That can't happen as long as the internet truly is some common space that nobody owns. As long as everyone views it as someone else's thing, you're going to take your sheep, and you're going to put them out in that common space and say, "Eat the grass," bring them back in at night, and harvest them, sell them, slaughter them or whatever you do to make your money off of them. They're going to eat the grass in the commons until it's gone.

Adrian Bye: Right, now I get it.

Jon Praed: To me, we've got to find a way to bring that border control concept…

Adrian Bye: …but without it becoming taken over by corporations. I mean ICANN is an organisation that should be strong in this area but in fact, they are fairly weak. United Nations is also not that terribly strong either, right?

Jon Praed: Yes. I think ICANN has challenges over whether their job is simply to make the trains run on time or to care about whether the trains are engaged in lawful commerce.

Adrian Bye: So your feeling is that ICANN should be helping developing this race to the top?

Jon Praed: Absolutely.

Adrian Bye: Indeed, are they not today?

Jon Praed: I think they're only beginning to understand that they cannot bury their heads in the sand and deny that they have a tremendously powerful role in enabling criminal enterprise.

Adrian Bye: Right.

Jon Praed: They are either part of the solution or by definition, they are part of the problem.

To give you an idea, the bad guy space is still in its teen years of maturing. The spam you get is almost always advertising the domain name, right. It's not advertising an IP address. It's got a domain name in it. That domain name was purchased by someone in the end accredited by ICANN, right? There are a relatively small number of bad guys and enablers out there selling thousands of domain names a month to these bad guys that are all known within the ICANN system.

Adrian Bye: So it's basically the same as affiliate marketing. You've got to know who all the people are and the banks have to know your customers. You're saying it should be the same for domains?

Jon Praed: Exactly and we haven't yet gotten to the stage where we've made it hard enough for them to buy domain names that they no longer do it and start dealing just in IP addresses.

Adrian Bye: That seems blindingly obvious. Is that not an argument that you can make very easily to them?

Jon Praed: You can make it but they view themselves as having limited powers to do anything about it.

For example, there are…

Adrian Bye: ICANN – I mean they're the ones that control the domain name infrastructure on the internet and they say they don't have the power.

Jon Praed: Yes.

Adrian Bye: I mean if they don't have that power then who does, the Department of Defence?

Jon Praed: That is why I say in the next 10 years, I think we're going to see a nation state division in the domain name space.

Adrian Bye: Right.

Jon Praed: I think the United States Government and other governments that understand the coming battle need to define some internet space that they can control and declare dominion over it. If the US doesn't do it, China's going to do it. Russia. Someone is going to do it and once they…

Adrian Bye: So all these guys then get pushed to where they can't buy domain names anymore. So then, maybe they've got to steal their domain names or just mailed IP addresses and that's going to make their spam even harder?

Jon Praed: Right.

Adrian Bye: Yes.

Jon Praed: They can't get access to premium domain names that can be technologically distinguished from other internet data points and allowed through. It's like airports that have frequent flyer express lanes that let frequent flyers go through without being subject to all the physical searches that everyone else has to go through.

Adrian Bye: Right.

Jon Praed: Finding ways to create an efficient border that distinguishes between good traffic and bad traffic or unknown traffic.

Adrian Bye: Yes. So you've got proxy servers and everything else that can make that difficult but I get the point and the direction.

Jon Praed: Right and that's the myriad ways in which the law can provide feedback to these technical filters that can allow the technical filters to become more powerful and more efficient. It's inevitable.

Adrian Bye: Now you mentioned that you worked with companies having problems with their domains being spammed or their brands being spammed. What does that mean and how do you help?

Jon Praed: Drug companies, for example – we've got a current lawsuit pending. We've been doing about an 18-month investigation into the online world of counterfeit drugs and its assassinating world. But drug manufacturers in the US and elsewhere are obviously being inundated with bad guys that are either spam advertising or even buying paid advertising – paid AdWords on trademarked drugs and driving that traffic to websites that are fulfilling those orders but shipping counterfeit product to unwary consumers or to consumers who know perfectly well but who don't care because they're actually getting the active pharmacological ingredient. They're getting a generic from India or from China that may contain the active ingredient but was manufactured under a process that is not as carefully regulated for safety and efficacy as the systems we've created in the United States. Those drug companies, I think are facing huge losses and really losses of unknown size as these sales just disappear from their books. The criminal arm…

Adrian Bye: When you get in and go and help a company with that, how does that work? What do they typically pay you? What's involved? How long does it take? …all that sort of stuff.

Jon Praed: Well, we have two pricing models. We use our technology to grab the data in the first instance so we have feeds from public sector and private sector clients that tell us about these websites and ads. Then we basically spider the web, grab all the data we need to get identity. We triage that data, looking for commonalities and then through undercover buys, informal investigative efforts and formal discovery efforts that we launch using John Doe lawsuits, we'll issue subpoenas to the enablers, designed to work our way towards hard identity on who these bad guys are. We may identify their real names, their real bank accounts, their real domains that they're using. We identify the merchant accounts that they're using to process credit cards and we do that generic triage work on a flat-fee basis for our clients.

For example, for $5,000 a month, we will acquire the data about a particular drug, provide to the client our analysis of the top fingerprints that we see in that mass of data and show them a path to identity. They can then hire us to do the additional work required to chase that to fruition, to its conclusion. But we also provide them as part of our standard fee, access to all the other information we've acquired through any other work and I think that's what's innovative about the work that we do. It's that our clients agree that we can share data with all of our clients that we acquire about bad guys regardless of which client we acquire it on behalf of because our clients recognise and agree that cyber crime is a common enemy, and that they are best protected when they share information about their enemy across the space. The identity of clients remain sacrosanct. We don't identify clients publicly except when we're required to do so in filing lawsuits or through other means. Information about their relationship with the bad guy…for example, the fact that they may have been victimised on a particular date…will also remain at least anonymised. So we may tell Client X that Client Y was victimised by the same serial fraudster on the same day and approximately the same time so that Client X and Y can know that there's someone else out there that's interested in catching this person, so that they can each make the decision whether they want to join hands through us and either remain anonymous or actually identify themselves to each other and by combining resources, get to the objective of finding identity and coming up with a strategic solution to the problem far faster than they could ever do on their own. So it's our ability to share data across clients and yet retain the attorney work-product privilege and the attorney-client communication privilege that is one of the core values that we add to our client-base by allowing them to, in essence, report acts to us and empower us to catch the bad guy faster than anyone else can, and to do so on behalf of our entire client-base.

Adrian Bye: Does this end up affecting major brands like Zappos and Best Buy – all these big brands on the web?

Jon Praed: Sure. If you have a fraud problem, we have a solution that can help you.

Are you still there, Adrian?

Adrian Bye: Yes, I'm here.

Everybody has a fraud problem.

Jon Praed: To the extent they've got a fraud problem then we have a view into it that can be helpful to them. I think our solution is a longer term solution and so the return on investment is a longer term consideration for us. But when it comes to hiring law firms, I think most companies don't really even look at Return On Investment. They view this litigation as a straight up loss and I think that's the difference between the service we provide as a law firm and other more traditional big law firms. There it's just a financial drain and for us, we are offering an ultimate solution to the problem that, to me, is the only viable solution out there. Either you're going to start to address this problem using these techniques now or you're going to wait until your fraud problem becomes a larger percentage of your overall revenue or profit until you decide okay, I've now got to start paying attention to not just fraud but how do we fight the fraud. The answer ultimately is you've got to fight it strategically. Too many people…

Adrian Bye: Can I buy stock in your company because it sounds like you've got a very good business model there?

Jon Praed: Yes. Well, as I say, we're marrying technology with legal practice and there aren't many others that are doing that.

Adrian Bye: Do you have a tech team to back all this up so you could take a brand name like Zappos, for example, go and find the instances of where Zappos is being fraudulently used on the net, provide reports periodically like every couple of weeks every month, and then if there's some area that becomes a big issue, you can then step on that and they can retain you to go after it? Do you potentially collect settlements from these guys or do you just put them out of business?

Jon Praed: It depends. It depends on who they are, what we can do to them, what the client wants to have done. Part of the point is giving them the ability to monitor what their baseline problem is and who's responsible for it from an enabling view. Who's selling the domain names that are being used by the bad guys? Who's a record-hosting? Who's DNS-ing? Whose e-mail addresses are being used in all of these communications? Part of our process for a fixed monthly fee is to reach out to those enablers and recruit them to the fight, putting them on notice of the role that they're playing and laying out for them their obligations, saying they need to be sure they're getting identity. They need to be enforcing their own terms of service. They need to be investigating based on our complaints and reporting back to us on what they've done.

Adrian Bye: Do you just focus on e-mail? I'm getting a lot of IM spam at the moment. Someone's figured out how to spam hotmail now in a sense.

Jon Praed: Right.

Adrian Bye: Do you go after other stuff as well or is it just e-mail?

Jon Praed: No, we go after anything, any sort of fraudulent internet activity that impacts

Adrian Bye: So you're like a bad guy sheriff now, like a Wild West sheriff.

Jon Praed: In the private sector, yes, I think it's inevitable that, that sort of service developed and we're definitely in that space. We see value in providing that service and trying to encourage races to the top. What makes me feel good about all of this is that no matter how bad and corrupt some places become, I only need one good jurisdiction to provide me the legal resources and mechanisms we need to get at the bad guy.

For example, it's relatively easy to identify a victim. Let's say we've got a spammer advertising something and we want to get at. We identify an enabler in Malaysia. All I need to do is find a victim in Malaysia to justify filing a lawsuit in that jurisdiction to issue a subpoena to that Malaysian enabler to get from that enabler the identity they have on the bad guy and then bring that data back to the mother ship and use it worldwide…

Adrian Bye: So you're going and doing this stuff – filing lawsuits, subpoenas and stuff in random countries like Malaysia and getting that done. I mean how on Earth do you manage that all from the States?

Jon Praed: Well, it's not randomly done. It's done based on a strategic view that this enabler in this jurisdiction knows something that's going to be extremely valuable to our overall strategy against this bad guy.

Adrian Bye: Have you done that sort of stuff here in the Dominican Republic?

Jon Praed: No.

Adrian Bye: I know some of the stuff down here and it's pretty antiquated. Along with the language barrier and everything else, I'm impressed that you could even start to do that.

Jon Praed: Well, it rarely begins with legal process. Our practice again entails capturing the data and then working it through legal process. A lot of it's informal. A lot of it may be through undercover investigative efforts. There is a lot of activity throughout the world that lots of people are engaging in to try to acquire more information and marry that up against what else can be known. I think a lot of people hear the legal process. They hear us trying to bring the legal process to bear and they think it's expensive and you're just suing people. Lawsuits are the last thing we do – the last thing because it is not cheap and so when we do bring lawsuits, they're strategic in nature and they are generally designed to first get us subpoena power to get us at the underlying information that we need. Most of the enforcement mechanisms in the end that we see are criminal or even military in covert and there's no reason why this data can't be used for those purposes.

Adrian Bye: Okay.

We've covered a lot of stuff and it's been a really interesting call. Is there anything that we haven't talked about that you would like to discuss?

Jon Praed: I don't think so other than the election. Let's see how that turns out.

Adrian Bye: We'll know soon. People who will be hearing this interview actually well after the election.

Jon Praed: Right. So history will have been made by then.

Adrian Bye: Yes.

Jon Praed: Well, Adrian, I appreciate your time. This has been enjoyable for me as well and I hope your listeners find it valuable.

Adrian Bye: Thank you. Thank you again.

Jon Praed: My pleasure.