meetinnovators™
where the deals get done

Interview with Anne Mitchell from SuretyMail

Adrian Bye: Today I'm talking with Anne Mitchell from ISIPP and we're going to talk a little bit about the state of email today and some of the things that Anne's seen going on down at the shoots right there in the trenches of getting email through and quite a history of working with email. Anne, welcome to the call. If you could tell us a little bit about yourself and your background and then we'll go ahead and get started then that would be great.

Anne Mitchell: Well, Adrian, thank you so very much for having me. It's always a pleasure to work with you and I'm glad to be back. A little bit about myself, well, I currently run ISIPP which stands for the Institute of Spam and Internet Public Policy. We have an email accreditation program called Surety Mail which we use to help ensure that legitimate email senders are able to get their mail through to the inbox and that was born of by original roots in the email industry which is actually on the anti-spam side of originally In-house Counsel and the Director of Legal and Public Affairs for the very first blacklist known as the MAPS RBL. So, my background is very much helping to make sure ISPs don't have to deal with email that people had not requested, also known as spam, but in the course of my work I have also become very involved in helping to make sure that legitimate senders are able to get their mail through to those ISPs and that was because at a certain point in time, a quite pivotal point in time, I became almost painfully aware that despite the fact that the ISPs and the email senders, the email marketers, etc., seem to be at odds, even now…back then, years ago, certainly it was much more so…despite all that, I became aware that really they wanted the same exact thing and they were actually on the same side, and that thing that they both wanted was to not send or deliver emails to people who don't want it but to make sure that the people who do want a particular piece of email get it, that it gets through. So, that in a nutshell is my background that's what I do now.

Adrian Bye: Ok. I got a lot of technical questions to ask you but do you want to just tell us a little bit about where the industry's at? The company that you were a CEO of for a while, Habeas, which was just bought by Return Path, do you want to talk a little bit about what that means.

Anne Mitchell: Oh sure, sure, so I was one of the original founders of Habeas, and Habeas was original founded as a company that was intended to help distinguish spammers from legitimate email senders and in fact to then sue spammers using Copyright and Trademark Law. During my tenure there as CEO Habeas sort of evolved into primarily a company that would allow legitimate email senders to distinguish their mail from spam which then in turn would allow the ISP's to quickly identify legitimate mails send it on and then they could turn their attention and resources to the bulk of the balance of mail which are, of course, spam. I left Habeas about a year after which it's founded and that was in, I believe, 2004 that I left and had not had any relationship with it between now and then, other than to occasionally have people come to me to tell me stories about how it was doing or to have people I'd hired in come to me to purely talk to me. At that time, at present day, up until really the announcement yesterday, there were 3 primary, what I would call, full service email accreditation companies. By email accreditation what I mean is what we do at Surety Mail which is working with an email sender and then vouching for them to the ISP's and Spam filters and say look, these are good guys they're doing the right thing, they're not sending spam their sending mail that's been requested and you should deliver their email to the inbox. The ISP's appreciate that cause that means that they don't have to churn resources checking this mail. In other words, they don't have to run it through their whole gamut of spam filters just to determine at the end, oh this wasn't spam to start with. This way they could just put it right at the inbox and again to bulk those resources to dealing with the real spam. So, at the time up until yesterday, there were just three of us. There was Habeas, again which I have founded and left a year later, there was our Surety Mail service and then Return Path which has their senders full service. By full service, I mean we work with all the different ISP's, we offer a host or a suite, if you will, a different service all related to email deliverability. We offer delivery inbox monitoring, so you can see if your email has been delivered to the major ISP's or not, we offer email client rendering which means that you know that you can take your email, your creative that you're about to send out and see how it will be rendered by 20 different email clients so you know how it will look when someone at AOL reads it and how it will look when someone at Hotmail reads it and what would it look like in Outlook and then even on a couple of different mobile devices so we offer that, and all the three services were offering much the same sort of services.

Just sort of on a side note, there's a company called Goodmail which is slightly different and what they do is they work with some of the ISP they basically put a little widget in your email that displays at the end that sort of says this email has been certified by Goodmail but they only work with the ISP's that actually are set up to have the infrastructure to accommodate that widget and you could only send mail if your certified with Goodmail by either using one of their NTAs or vendors so they're not really full service in that same way and they don't offer other services but I mentioned them because often their name comes up as well and I don't want them to think I was snubbing them.

So there were 3, there was Habeas , ourselves, and Return Path and so what that means to get back to your question now is there are 2, they're…because Habeas is actually sort of being incorporated into Return Path. And I read..

Adrian Bye: So you're a stockholder still in Habeas?

Anne Mitchell: Yes, yes I was and that's a very Interesting question that everyone seems to want to know the answer to. Yes, I, of course had vested a year's works with stock, however, it's no secret at this point because there's an article written in the past 24 hours that brings this to light that Habeas was sold for a pitting. I'm not at liberty to say whether that pittings cover the debts which they were servicing but I can say because it has already been out there publicly that no one would even stop that for anything.

Adrian Bye: I thought you're going to be retiring to the Caribbean on your own Island that you bought?

Anne Mitchell: Well, I may still do that but I'm very happy to say that our Surety Mail accreditation service and generally ISIPP is doing extraordinarily well so if I do in fact retire to the Caribbean it would be from the fruits of my own labor here, and of course the company, not just me you know we have a wonderful staff, but it will be a function of the current company not my stock at Habeas. Let me say this, because this is very critical, not that I think necessarily it's important for your particular listeners, you know, they may or may not care about how I feel about the ultimate disposition of Habeas, but it's important for me to say this, and I've said it in interviews and I'd like to say it here because we're on the subject. People have wondered how I feel about what was originally, my baby, Habeas, being acquired by what, in essence, the competitor, and I'm really very pleased. For one thing, Habeas also had become a competitor and in fact, I think, they saw, quite seriously, as a competitor, and thought that perhaps we were a challenge to their model. On the other hand, they also had copied something we had done once we came out with some innovative features and I had anticipated that and so I took that as a complement so we were competitor but also an acknowledge innovator there, but in any event, I feel very good about Habeas being acquired by Return Path primarily because when I founded or co founded Habeas, it had a great deal of potential and during the time I was there, it had evolved in a direction that really held promise for both sides of the equation, both the email receivers, the ISPs and spam filters, and the email senders for getting legitimate mail delivered. As I have been quoted saying in an interview, the Habeas that Return Path acquired was not the Habeas that I founded.

Adrian Bye: Right, it must have changed a lot over the years. Look, actually, what, this ties in a way to what I wanted to ask you some questions. Because there's innovation coming up in the email space there's some…I haven't been tracking it that close in the last year or so but I know there are things like SPF and domain keys, those kinds of protocols are taking tolls with…email can be authenticated based on domains and things like that. Given that Habeas as one of the major players in the authentication space has been acquired for not entirely a large amount of money, does that put some sort of a level of indication as to the importance of the space? I mean how important today really is accreditation given that we have all these other sort of protocols coming along for authentication?

Anne Mitchell: It's extremely important and let me just finish, please, what I was saying because it was critical and then I will address that, and I just wanted to say that I'm very pleased that Return Path acquired Habeas because I know the people at Return Path and they are stand up people and I know that they'll do the right thing. So, I'm very comfortable with Habeas now being in their hand, I just want to get that out there because that's really what people wanted to know when they were asking me these questions.

Now, about authentication and accreditation, you know, I don't know if you've been provisioned any of the discussions or any of the mailing lists, or what have you's, involved in the development of the authentication standards, or indeed any standards. If you've ever sat in on any of the IETS working groups, then you know

that every great idea has its gear, I don't mean it last year, I mean it takes it that long to get to a point where people can agree about anything about it. There are some promising authentications out there but there is by no means widespread, let alone, universal adoption for any of them. I mean, SPF has been around for how many years now, and we, have people come to us every single day, applying to get accredited, who not only don't have SPF set up and they know that they probably should but they have no idea how to do it. In fact, just this week we launched a service with which we will set up your SPF and domain keys for you because so many people have no idea how to do it. So, the adoption by the actual people who need to use it, the end-using email senders, there's just not the uptake to even get close to universal for any of these mechanisms. So, they are very important, and any upcoming system will also be very important. When I say very important, I mean that there are huge ISPs that if you are not publishing SPF or domain keys, you're probably not going to get your email into those ISPs or at best you're going to get into their junk folders. So, it's extremely important but despite that, the message and the adoption just haven't followed. So, the technology, these innovations are important but they do not, and I would say even unfortunately, obviate the need for accreditation. And when I say..

Adrian Bye: If they're not adopting free things like SPFs and Domain Keys, why would they be more likely to adopt authentication in paid services like yours?

Anne Mitchell: Because, we'd take care of everything for them. For the most part, the typical email sender, and I would say the majority of email senders would…there are rare exceptions some of the very large ESPs who have their own in-house people. But the typical email sender really doesn't know how to go about fixing the problems they have with deliverability. You know, they don't know how to set up their SPF, they don't know any of those things, and even though they're basic of things and they especially don't know how to and probably are not in a position to develop the relationships that they need to with their counterparts, with all the ISPs, whereas the email accreditation programs are solved in Return Path both. Already have this relationship with each of the ISPs. So, for example, Adrian, if you suddenly woke up tomorrow and found that all of your email had been blocked at AOL or Yahoo or even just that it started going into junk folders, would you know what to do? What would be the first thing you'd do when you realize that?

Adrian Bye: Call Anne Mitchell. No, I'd send her an email. I personally realized a while ago that email is too hard even, and I think I have a moderate understanding of it, and so I do my email on Google applications now

and I use mailing list services to deliver my list emails. So, in those situations I have people to raise it with on either side and those people who are more educated on this than me can get in and solve the details.

Anne Mitchell: We see in that exactly that you really just answered your question. That's the answer to your question. Because people would want someone who's already got the contacts and already knows how to do it for them. And in reality, for most situations and most senders of any size, its more cost-effective to do so. Certainly, we are extremely affordable and if you think about what your time is worth and if you think about the learning curve and once you've learned to do all these things and once you've made all the connections with the ISPs and spam filters, if in fact you can, then there's still time once you've learned all that, that it takes to apply it, every week, every month, everyday, what-have-you. So from sheer cost-analysis, it's much more cost-effective to pay someone to do these things for you and to make sure that your email gets delivered, and of course let's make no mistake, for many, many companies now email is their financial life-blood. If their mails are not getting through, they're not earning money.

Adrian Bye: Correct. So if I come to you…let's say some people want to use a service like Exact Target which has fairly high rates on a per CPM basis to deliver email, I could then have all my mail housed internally on my own mailing software and then handle the deliverability myself. With you guys as the backstop to get the mail through, and so then as you said, I wake up one morning and my mail is not getting into Yahoo, I can call or I can email you guys and you guys will look into it. Is that basically how it works?

Anne Mitchell: So now, if you're using Exact Target then your mail is going out through their IP addresses. Now, I'm happy to say that Exact Target actually is accredited with us, so you should have no trouble if you're using Exact Target. But generally speaking, of course, all primarily, its changing a little bit now. Overwhelmingly still, email verification is based on the reputation of your IP address. The IP address from which your email flows. So, if you're using an email service provider such as Exact Target, and of course, there are many other fine email service providers as well, then your email deliverability is keyed directly to the reputation of the IP address at that email service provider through which your mail goes. Now, many email service providers, particularly, many that work with us because we really urge them to do this, will give you your own IP address so only your mail is going out through that IP address but with many other email service providers, your mail is going out through the same IP address as a hundred other companies, and if any one of those companies sends out a spam, suddenly, your mail is going to get blocked, too, because its going through the same source.

Adrian Bye: Right. But they're monitoring that. So, let's just say if I'm using Exact Target and Exact Target is managing all the mails for me and handling the deliverability, and then I go use my own internal mail service is that when I can have you manage my IP addresses so that if problems come up with my IP addresses, then you go and sort it out with your ISPs. Is that how it works?

Anne Mitchell: Essentially, yes. Just to clarify what you're saying, say you're using an email service provider such as Exact Target, and then for some reason you choose to stop using them and to send your mail out through your own mail server, yes, that's exactly one of the times when you would come to us. Ideally you would come to us as you are making that decision so that we can counsel you on how to start out right from the beginning doing everything right because it's so much easier to start with no reputation and then build it up than it is to start to rehabilitate your reputation because you unwittingly done something wrong. And I

have to tell you, and I don't know if you read my…We have an email deliverability blog at gettingemaildelivered.com where that's what we talk about everyday, the things to do right, the things to do that can be done wrong that can affect and impact your email deliverability, and quite relatedly, today's post was actually about how just the content you choose can either cause your email to be delivered as it should or to go right into the junk folder. So ideally..

Adrian Bye: Is it going to make that much of a difference?

Anne Mitchell: It makes an enormous difference.

Adrian Bye: At what percentage of the overall importance would you place the contents of the IP addresses above everything else?

Anne Mitchell: Well, you're going to be glad to hear that I'm not an accountant when I tell you that I would say that its 90% to the IP Address and about 90% to the content. And you'd say, how could that possibly be? That's why I'm not an accountant but let me explain. It's not an aggregate, primarily, in terms of, you look at IP address, is it good, or you look at the content, is it good, its rather a series of steps. The IP address reputation is what will get you past the initial check. In other words, if your IP address is in a blacklist, your mail will never make it in the door of the ISP. But once your mail does make it in the door, then you have to run all the spam filters which look at the content and the other things. So, both are necessary but neither alone sufficient in terms of getting your mail delivered.

Adrian Bye: That's interesting because I thought that content had become much less important and I thought we were doing a better job on filtering based on the IP addresses and stuff like the domain keys now and so, that that was what they mainly look at. So, I guess, I was pretty wrong.

Anne Mitchell: I think that you're probably not wrong because I think you're probably talking about something slightly different from what I'm talking about. Or maybe we're totally at a sort of bi-phase sort of thing. It is true that the decision about whether to accept email at all into a receiving system is still based for a large part on the IP address and authentication. But again, once it's accepted in, rather than blocked or bounced, the decision if whether it is going to get delivered to the inbox or the junk folder, is extremely keyed to content. So, you might be talking about blocked or bounced, versus junk foldered. I'm talking now about junk folder versus an inbox.

Adrian Bye: Right. I guess...Ok, let's see some questions. Actually to that point then, I'm interested in how Google Apps generally does a pretty good job with its spam filtering. I get about 2000 spams a day now and it's increasing. If you could buy stocks in spam I'd certainly buy them because it just goes up and up. They do a really good job in filtering and my guess is that they're doing some kind of collaborative filtering to keep your mail out of the inbox. Do you know anything about how Google Apps filters?

Anne Mitchell: I know pretty much what everyone else knows which is a great deal of speculation, very little confirmation but its educated speculation. I would agree. You know, of course, they have Gmail in which to draw and every time you click at something that's spam, a hundred thousand other people click the same thing as spam, it would only make sense they would use that data to educate and inform their own spam filtering decisions. Now, again, no one has actually ever confirmed that but it only makes sense. Interestingly, however, I would say that their false positive rate is not stellar, it's not awful, there are places that are worse, but you know, of course, and I think we've talked about this in the past, that, you know, the better and more effective your spam filter is, the more likely it is to also, being a spam, identify spam mail, that you know, use a spam that you really want. That could have some really dire consequences particularly for transactional emails. Not so much for bulk email but the reality is that if you don't get the particular issue of a newsletter that 500,000 other people are also getting…It's unlikely that you're going to be terribly impacted by that in any negative way, but if on the other hand, you don't get a notice of an appointment or a confirmation of a travel arrangement, you know, something that's a transactional email, it could be absolutely devastating and we heard stories of lawyers who have missed Court dates to the detriment of their clients because their spam filter ate the hearing notes that had come from the Court.

Adrian Bye: That's interesting. I mean the way I get to do that, I handle that with Google is I do a keyword search for my first name and last name and then some other related keywords of the things that I'm doing and I set that on my spam folder once every couple of days and then the important ones comes out and the rest gets deleted. I don't find too much that way, I know I do miss some messages but in general I haven't missed any Court date.

Anne Mitchell: That you know of. Well, and see, that really raises a good point which is also a point that's raised every time we talk about the Court date story which is its almost, well I would say, speaking as a lawyer now, and now that people have noticed, in a legal context, I would say, that it is almost rises to malpractice to not check your spam folder if you know your local Court sends notices by email. So, the metapoint there is that no matter how good a spam filter is, you're still going to have to look through your spam.

Adrian Bye: I mean, I'm getting 2000 a day so I'm not willing to do that.

Anne Mitchell: So, you are looking. By looking through it you are checking it, you're still doing a form of checking it. You're doing a sort of a more high level form by doing a search and that..

Adrian Bye: I'd make a suggestion to you, I sent that suggestion into Google that they received but didn't act on. I believe that all of the services should enable you to do to specify some keywords that you're looking for that goes in the junk mail and then automatically give those as white list to get to the inbox. In that way, if you could just specify the keywords that they're looking for, that's going to reduce the spam mail. And that's also something that spammers are not going to be able to figure out and if they do you just have to change

the keywords. Given that you know some of the right people maybe you could start mentioning that sort of thing so that they do that.

Anne Mitchell: That's a very interesting idea. You know, I mean in native spam filtering, some of the email clients can already do that but you're absolutely right that for the ones that are web-based or off-site, that's a very interesting idea. And you're also right that the spammers would start screening it.

Adrian Bye: Yes, it will get gained. When you can set the keywords yourself. Anyway..

Anne Mitchell: Right. Actually I have a question for you.

Adrian Bye: Tell me.

Anne Mitchell: You mentioned that you mind your spam folder by searching for your name, and often spammers would have your name because they've purchased a list and so I'm just wondering if you have found that do you find that search terms that many thinks that are actually still spam and you sort of just look at them in disgust and say, well I can't believe you've used my name, you bad person.

Adrian Bye: Well, they don't tend to have both my first name and my last name in the spam and then the number that comes up in my, out of the 2000 that I got that day there might only be 10 or so that's a quick read.

Anne Mitchell: Ok.

Adrian Bye: I guess it would have to be scanned manually. Good point, because I wouldn't want all of those to get to the inbox, but the volume's a lot lower.

Anne Mitchell: Right. Because it's only a certain, you know, section spam that also uses your real name.

Adrian Bye: Right. Exactly. Good point, so I guess that maybe, my spam volume is getting very high and I can't process all of that manually. The other thing that I wanted to ask you about is the different mail services like Hotmail, Google Apps and Yahoo, and then AOL, that would cover the big 4. Who would you say is doing the best job in processing and filtering spam?

Anne Mitchell: Processing and filtering spam, keeping it out of the inbox of their users or processing, filtering, and keeping it from being sent out to others?

Adrian Bye: On the users' side, doing the best job at blocking spam and also on not having false positive.

Anne Mitchell: I have to say that Google does a pretty good job, now you're talking Google Apps and I'm talking Gmail I have not personally worked with Google Apps but of course they're built into some extent the same platform as far as I know. I can say that Gmail does a pretty darn good job on keeping the spam in the spam folder. Their false positives are not awful, they're not great but they're not awful. AOL we hear very few complaints about.

Adrian Bye: So you're number one would be Gmail and number 2 would be AOL.

Anne Mitchell: I think so. But you know it always changes and part of what informs that is every user has a unique experience because they're receiving a unique mail stream. Right, so if you have an AOL account and you're signed-up to a lot of newsletters that have to deal with, oh I don't know, herbal products, you know you're going to tell me that the false positive rate is absolutely appalling because they are all going to go to your junk folder. On the other hand, if you're maybe sort of an older retiree and really all you're using your email accounts for is communicating with the kids, and you do very little commercial transactions online so you're not really expecting to receive anything that's bulk or transactional you're going to tell me that, boy, AOL is wonderful because they never get it wrong. So even there it's pretty really hard to quantify and everything is anecdotal.

Adrian Bye: I was actively testing different mail services a few years ago and I used a lot of tagged email addresses so I could tag them and send them into the trash. Since I've moved to Gmail, or Google Apps, all those filtering are now gone but Google Apps is actually just classifying them all themselves and they're doing a really good job. I was a little bit stunned, I thought I was going to get overwhelmed with spam, but they're actually getting it most of the time right like 99% right.

Anne Mitchell: Now, I'm not surprised to hear that.

Adrian Bye: You mentioned briefly and we should talk about that. You're a lawyer and you've been involved with the legal side of cam spam and you in fact helped off some of the cam spam order, is that correct?

Anne Mitchell: That's correct.

Adrian Bye: I know that there's some changes happening in the law with regards to email and I know that could be a long topic in itself. Maybe if you can just tell us a little bit of what's happening there. My impression is that basically it's changing almost nothing, is that correct or am I misguided?

Anne Mitchell: Now, I'm not sure I understand the question, so are you saying that, despite having the law, the new laws or revision to the law that the spam landscape is still the same?

Adrian Bye: No, that the legal perspective like cam spam, that the update that's coming through to cam spam is…it's either happened or it's about to happen, or it doesn't change much.

Anne Mitchell: No, actually it changes quite a bit. It has, and actually, I'm going to make sure that I don't misspeak so just hang on just a minute here because what I want to do is pull up so I have it right in front of me, so I don't misspeak or forget but there's four primary new changes, if you will, to the law and by far the most dramatic…actually let me start with the simplest. First of all, it clarified, and so in this way, you're right, that in a peculiar aspect the law didn't change much. Yet one of the things about cam spam was that it required that you put a physical mailing address in each and every bulk or commercial bulk email that you send. When that first was enacted, we had people coming to us, all up in arms, very eager to learn, because what they wanted to know was does this mean we actually have to put our physical address where we sit in our office or is it ok to use a post office box, if it's a legitimate post office box in which we really get mail. Our advise to them at that time was, and that came from my legal background and knowing how the legal system works generally, and knowing also what a monumental task is at the FTC, the Federal Trade Commission has in going after spammers. Our advise was look, if you're doing everything else right, and you choose to use a Post

Office Box as your mailing address in your cam spam compliant mailing, then FTC is not going to come after you for that. They have much more important things to do than to go after someone who's really trying to comply and do everything right just because they put in a PO Box. You know they have much more important fish to fry and not..

Adrian Bye: You're saying in theory we're now supposed to put our physical address where we're sitting at the time we sent the email?

Anne Mitchell: Excuse me?

Adrian Bye: In theory, we're supposed to put the physical address we're sitting when we send an email?

Anne Mitchell: Well, in theory at the time, that was certainly how it could be read. But it was gray. So, one of the clarifications that came down this past month was that, yes, in fact, you may use a Post Office Box. So, what we had told people it basically just confirmed. So, it's no longer theory, its confirmed, you can use a PO Box as long as it really is your PO Box that you exercise, control, and you really go there to check the mail.

Now, the next thing that came up that was clarified or amended this past month was that, you know, as everyone already should know, you're required under cam spam to remove an email address from your mailing list within 10 days of refusing that request, the request to opt out. Many people will argue, I think, perhaps rightly, that 10 days is an awful long time and we tell people you should remove it immediately. You know, the moment someone tells you that they don't want your mail, you should stop sending it to them because you're only courting trouble, otherwise.

Adrian Bye: I think the 10 days rule is perfectly reasonable for the 1960's when you got big mainframes running COBOL. I think that would be actually fair, if someone is going to carry the tape from somewhere to somewhere else. I can't see how anything under instantaneous is acceptable for that.

Anne Mitchell: I absolutely agree. Now, I know that part of the reason the 10 days initially came into play was because there were senders who often cue things up days in advance, so, it's already in the pipeline and their concern was that they would people would then get something after opting out and suddenly they'd be in trouble under cam spam but really that talks more to process than to the removal of the email address, and so even though, again for that reason you have these 10 days you absolutely ought to be removing that email address from your mailing list immediately. Now, what this clarifies, this new rule clarifies was not how much time you have to do it, which stayed the same, but how onerous that removal request can be and that can be not onerous at all. What the new requirement is that the act of opting out, must only take a single action. So, for example, when I click on my, you know, on the little link on your email that says "unsubscribe", it must take me immediately to the Unsubscribe…We would argue to the "You have successfully unsubscribed" page. We would argue, we counsel senders, you definitely should not be asking them for a password, that's just not ok. You definitely shouldn't put an intermediate page that says, "Are you sure you want to unsubscribe? Here, let us tell you all the reasons why you shouldn't and arguably it shouldn't even be a page that says, "You are about to unsubscribe. Do you want to confirm?" You know ideally, a single action means when I click unsubscribe on that email, I'm taken to a page that says, "You have been successfully unsubscribed." Now that page can say, "If you didn't mean to, click here." But effectively..

Adrian Bye: I love those ones where you have to login to unsubscribe, and so then you've forgotten your username and password on that site, and then when you try twenty different things to get it to work then you go to the section where you unsubscribe and you can't find that in the user or the site, that's great..

Anne Mitchell: Absolutely. Or even better are the ones where you never even registered a password, they just assign one to you that they never told you about. So this is the deal with all of those. Ok now, so those are pretty straightforward. However, this last one that I'm going to tell you about is the one that is just confounding. It is the most…now I have written legislation which I like to think is fairly straightforward. I always try and write in a way that, while legally tight, non-lawyers can understand. I will be the first to decry and have indeed done so, legislation that is just impenetrable. But I have to tell you that this new "clarifications" to cam spam, is perhaps the most confusing, confounding, impenetrable piece of legislation I have ever seen. So, when end-users, and email senders take a look at it and run screaming, it's quite understandable, because it took me several read-throughs to really grapple what it was saying, so here you go. This by the way is up on our website. We have a very straightforward cam spam compliance page which really breaks this down. Perhaps the best way to explain it is to explain what it's trying to avoid. You know those cases where you get email from someone? Let's say you get email from Suretymail.com, ok, that's who sent it to you and you look at the sender and you go, "Ah, Suretymail is sending me email." Then you open the email, and the only thing in that email is a big old advertisement for FedEx. Right? Maybe FedEx paid us a bunch of money to say "Hey, you know, you guys ensure it positively gets there in the inbox and we positively sure get real packages there overnight so there's a synergy" you know..

Adrian Bye: That's called a solo mailing

Anne Mitchell: Alright. Now, you're the end-user, who do you unsubscribe with?

Adrian Bye: I unsubscribe from the ISIPP list.

Anne Mitchell: Ok. Who do you think the average end users you're going to try and unsubscribe with? Do you think they'll know? Do you think they'll look up at that header or are they going to see FedEx?

Adrian Bye: So, the user wants to unsubscribe from the FedEx list.

Anne Mitchell: Do you see how there can be confusion there? So, this new rule with cam spam is to help address the confusion that things like that cause. So here's the rule. If you send email that contains advertisements for entities other than yourself, so third party advertisements, one or more doesn't matter, you must also include some sort of advertising text for yourself in that same email. If you do that…

Adrian Bye: Why do they do to stuff like this?

Anne Mitchell: Wait, let me finish. This is a tripartite rule. If you do that, if you be sure to include that text for yourself in the body of the email, you become what is known as the designated sender so this is called the Designated Sender Rule. You then are the designated sender for handling opt-out request. If you fail to include in the text, the body of the email, something about yourself, then every advertiser who has advertised in that email is on the hook for handling opt-out request.

Adrian Bye: Why are they making it so complicated when...let's say I get the FedEx team out from the ISIPP list and there's just an unsubscribe link at the bottom, I just unsubscribe from your list, I never get solo mailings again and so we've taken care of it. Why are they complicating the issue in that way?

Anne Mitchell: That's a very good question which I hope you would be able to ask someone else that you will interview that will be able to give you better insight there other than to say that this is usually, well, you know that old saw about you should never watch self into our legislation being made and you can imagine that as these things were coming down the pike, and I'm sure you know that there are always hearings at which email senders, email service providers, ISPs, etc. all get to provide input and then hopefully the legislation committee takes into account all that input. I can only imagine and I honestly don't know because I was not at those hearings that they heard so many different conflicting things that this is their best effort to protect both the end-users and the senders and the advertisers. Because you know..

Adrian Bye: You have one more to explain to us don't you? So, maybe if you can do that because I then have some more questions around just the legal side of this so if maybe we can do that given the time constraint.

Anne Mitchell: Actually, the fourth one was just a sort of a reiteration as to who cam spam applies to and that's to any and all commercial bulk mail. What does that mean, that includes email for which your primary purpose is to feature or sell your own goods or services even if you don't send that email yourself. Really, that second one goes to the McCain Amendment which is what the legislation that's a part of cam spam that I helped to author which is a whole other area. The fourth one really was, in fact, I was hoping that you wouldn't remember that I said 4 because it's really a non-issue, it just confirms what was already in place.

Adrian Bye: Ok. So the point is, there's a clear issue around and we talked about it several times, now I still, I don't get.. I'm not really happy with the conversations we've had because I didn't get an answer that I really understand. There's a real problem with people being able to go to a site and sign up and the privacy policy in tiny words saying, like an end-user agreement that says, we now have permission to resell your email address to every single person we like and they'll be sending you email from lots of different addresses, and so therefore, your email address is now done for because we're going to send you so much spam. It seems given that third point that you highlighted in this law that they're deliberately trying to enable this kind of stuff, and all these solo mailings and everything else that happen. Why is this sort of stuff being enabled instead of just stopped?

Anne Mitchell: I actually think that they're trying to not disable it but they're trying to make it very onerous. Right, and here's the reason. As an email sender, if you are FedEx and you come to me and say, I want you to do this solo mailing, I know the headache that's going to ensue if it really isn't solo mailing. I'm going to say no, and actually, probably you're not going to ask me to do it now because if it really is a true solo mailing and I am not featured anywhere in the content, the headache is on you now, the burden is on you. Right, because now you're going to be on the hook for all those unsubscribe requests as well as me. So, I really think that this was an attempt to put control on something that really had become out of control as you pointed out, the potential there. I think it might have been not the best effort that could have come out of that, it might even be misguided but I think that the intentions were pure and I think really it's an effort to..

Adrian Bye: That's alright, I think their intentions are really poor because it seems to me they're enabling something that shouldn't be allowed. Why aren't they just making some sort of rule that says, if you want to

have someone signing up for an address, the from address the mails will come from have to be clearly and conspicuously displayed. If you ever choose to display that, you may change that from address once a year and then everything will be clear to everybody. I mean, if they're..

Anne Mitchell: It's already the law that you're From address have to be clear so I think perhaps I did explain something wrong, maybe you're thinking this all have something that doesn't..

Adrian Bye: No, it allows reselling of data.

Anne Mitchell: No. No, it shouldn't. I'm not following..

Adrian Bye: There's a big industry around this kind of thing where I can, let's say, everyone who joins up to my list, to Adrian MeetInnovator's interview list, gets an interview, I could have in my privacy policy that I also agree to, you'll be getting emails, and you'll get automatically added to Anne Mitchell's email deliverability list. So, everyone I meet automatically goes on to your list plus 20 other different companies.

Anne Mitchell: But the emails that they'll get from Anne Mitchell's email deliverability list then will be from Anne Mitchell's email deliverability list it won't be from Adrian Bye.

Adrian Bye: Right, but I'm legally allowed to resell all of my data to you.

Anne Mitchell: See, that's why I said I think you took this to a different place. What I just talked about the new rule I just described does not address that at all and has nothing to do with that whatsoever. In fact, quite the opposite, this rule addresses when you take the list of people that you have and you don't sell it to me, instead, you send them email advertising me. That's what that rule addresses.

Adrian Bye: Yeah, fair enough. I guess to me it's hard because that's how they use the data's end-result for the solo mailing. But yeah, I take your point.

Anne Mitchell: But let me just say that I absolutely agree with you 100% and, you know, we very strongly discourage and indeed will not accredit someone who has agreed privacy policies like that and I would in fact... the problem with those privacy policies they have so much fine print as you pointed out. Can I take just one second, I'm sorry, less than 10 seconds…Can I read you our privacy policy? It's that short. The ISIPP SuretyMail Privacy Policy is very simple and I'm quoting now, "We will not share your private information with anybody ever absent your permission or Court proceeding which compels us to produce such information." That's it. And you know what, that's what a privacy policy should look like.

Adrian Bye: Alright.

Anne Mitchell: So, we're in complete agreement.

Adrian Bye: We are. It's just that the FTC and the government isn't and they're enabling a lot of these stuff. I mean cam spam came out a long time ago and it's still there so I don't get it. It seems like these guys are just on a different planet.

Anne Mitchell: As well as you know, Adrian, in the U.S. our email policies are all opt-out and the E.U., and England, Britain in particular, have much more strident email policies that require, first of all, opt-in, and

secondly the penalty, their privacy policies, their National Privacy Policies are so much tighter and there's a huge penalty to be exacted if you reveal someone's private data without their permission.

Adrian Bye: Ok. The other thing that I wanted to ask you about is just in general, and let's just back in onto ISIPP, if I didn't want to use ISIPP and I just wanted to do domain keys, and I wanted to do FPS, if I have my content right, domain keys and FPS, is that going to get my mail through or do I still need to have some sort of certification?

Anne Mitchell: That's a good question and there is a straightforward answer for that, and that is it depends. That's because every ISP is different, every spam filter is different and every mailing footprint is different so the answer is absolutely, yes, that could be all you need. It really depends on what you're sending out, even if you're content is completely right, it depends on your profile. How much you're sending out to how many people, in what frequency, etc. It depends on who you send to. For example, some of our senders, their mailing list is almost entirely Yahoo, or AOL addresses, for example, and so in that case, what they need to focus on is very different than if they're mailing list were primarily, you know, people at enterprise, you know, B to B, for example. So, it really depends but it will certainly not hurt and it could get you a large part of the way there. Also, just for your own sake, of your tiredness of your mouth, you can stop saying ISIPP, you can just say SuretyMail, which is the name of the service. Isn't that easier?

Adrian Bye: Fair enough. I've got a couple more quick questions.

Anne Mitchell: Sure.

Adrian Bye: I've been asked with one mail service that I'm going to be using. They say that to use their mail service, I have to use a sub-domain or a domain through them. So, they want to send a mail from their own domain so that then it's checked, what they offered me as an alternative is to register my own domain and have, or a sub-domain, so it could be mail.mydomain.com and that would be exclusively used by them. They said that it's the only way to get mail delivered now, and if any service is mailing under your name, then they're deliverability is going to be significantly worse. Is that correct?

Anne Mitchell: Wait, let me repeat what I think you said. So you're talking to an email service provider, right? They are saying, either, let's call them MailDelivery.com, they're saying either you need to have your mail go out under Adrian.MailDelivery.com or you could set up mail.adriansaddress.com and that will be what they will use to send your mail out.

Adrian Bye: Exactly. Whereas other services will happily go along and use my email address as I specify it and it seems to work fine.

Anne Mitchell: Ok, what they are saying, first of all the piece that is missing there is undoubtedly the reason that they are saying that is they want to assign you your own IP address and to assign you your own IP address they need to give you a unique domain that goes with that IP address, right?

Adrian Bye: But they are my mail from their domain, so it's either their domain or my own.

Anne Mitchell: Right, right but they're almost certainly doing that by assigning you your own IP address and they're absolutely right that that is the best way to ensure optimum deliverability. Is it the only way? No, but

it is certainly a best way, just as if your sending your own email out, not through an email service provider you will be presented to be doing it through your own IP address and as I mentioned earlier really it's critical that if at all possible you send your email out through a dedicated IP address that only you are using, so this email service provider is actually telling you truthfully what the best practices are, now, it may be that that is the only way they would do business and that's certainly their choice and it would one we would applaud actually because again it really is best practice, but it's certainly not the only way and absolutely you can go to other email services providers that would do it differently.

Adrian Bye: Ok, the last question then that I wanted you to ask about is in sending an email, let's say, this maybe not a small question but maybe you can give somewhat of a summary. If you send an email from your server to AOL, Hotmail, Yahoo or Gmail, what are the current checks you know that an email goes through to get in to the inbox?

Anne Mitchell: The first thing that happens is that their receiving server will make note of the IP address from which you're connecting. Then, it'll do a series of checks on that IP address. The first thing it will do is look it up in all the different black list and see if you're listed there. The second thing that may or may not do is look you up in the various accreditation services such as ours to see if you're listed with us. Then, and now I'm sort of aggregating, this is a combination of all the different things different ISP's do, then they will check to make sure that you have RDNS which is reverse DNS setup and that means taking your IP address and seeing what domain claims to be serviced or that IP address says it services, so it will check to make sure that your IP address resolve back to Adrianbye.com. Then it will look at the email the headers of your email to see, okay this IP address says it's Adrianbye.com so who does the email say it's from, it'll check to make sure that the mail is coming from the domain Adrianbye.com. Because, of course, spammers always spoof their emails, so, if, for example, your mail is claming to be from adriabye.com but the IP address actually resolves to example.com, the odds are good that your email is either going to get bounced or blocked or going to the junk folder because now you're sending email claming to be one place but really the IP address is another. Okay, are you with me so far?

Adrian Bye: Yes.

Anne Mitchell: Ok, that's all before their server ever accepts your email into their mail server. Once it passes all those checks, then it goes into content filtering, and that can mean the actual words and phrases you're using, it can mean domain to check to see if you have links to domains that might be on black lists with because maybe someone who is sending a lot of spam advertising from a particular domain.

Adrian Bye: before we get to that level, I know one of the things they used to be able to white list mail was if it's from a friend who is already in your address book and that would bypass all of those filters, and therefore, tell-a-friend got through. Is that still the case, or not the case anymore?

Anne Mitchell: No, and that's actually content filtering at either level, so that was not before got accepted into the server. There will be no way for that to be the case. Unless, now again that depends on what you're talking about mail that's hosted through an ISP or mail that's on your mail server, certainly you can put whatever rules you want in your own mail server, but I do not know of any ISPs that actually take their users address books for white listing and put that out in front of the mail server. I mean that just wouldn't even...

Adrian Bye: What you're saying makes sense, so that's called content. Fair enough, I didn't realize that.

Anne Mitchell: I'm just including that as part of content, in other words, you know the whole headers and body of the email now, content typically has meant in the past, does it have the word Viagra in it? Or whatever but in this context, I'm talking about everything from the headers down to the bottom of the email, you know, it's all text of one form or another, right, and the spam filters are all looking at what's in that text. So, again, it's looking at the URLS that are in the text of the email, domains that are being advertised in the text of the email, it's looking at the from address and its even looking at the to address, and it's looking at the subject line and it's looking at the overall content of the body. It's looking at the HTML to text ratio, it's looking at the image to text ratio, it's looking at the size of the font in the HTML and it's looking at all the words in the body of the email. All of those things are being analyzed by probably at this point all of the ISP's in one way or another and all of those things can determine whether you get delivered now to the inbox or to the junk folder. Once, you've already been accepted into the mail server, your mails usually are going to one of those places, either to the inbox or to the junk folder. Now, that were your white listing based on the from address comes into play. Does it go to the inbox because you've white listed that address or does it go to your junk folder? Now the other thing that some of the ISPs and spam filters, particularly ISPs, are looking at now is your open rates and click through rates. So if you send 500,000 emails to many, many people, and if not many of them are getting opened, then you're going to start going to the junk folder because the ISPs is going to see…

Adrian Bye: So, they're putting a pixel to track open or I guess they can easily see whether the users open. Are they cloaking the click through URL so they can see whether people click on stuff?

Anne Mitchell: I can't comment on that, and I do not know of any ISP's that are openly doing that. But I do know that there is the ability to track a click through. Now again, I have to caution to say that when it comes to open rates and click throughs, I'm talking about webmail, we're talking about places where you go to their site to look at your email. Because that's the only way they could track it, they certainly can't track it once it's been downloaded from their server on to your computer.

Adrian Bye: Right.

Anne Mitchell: But that's one of the reasons we caution our…we work very close with our accredited senders on these things to make sure that they understand the ramifications. It used to be you just didn't really care about open rates except that you know it was something you could advertise to your customer, come with us because we have great open rates. But now you really need to care about those because they can affect your deliverability, and so really, all this really means is you need to care that what your are sending isn't junk. You need to make sure that what your sending your users want and that it is compelling so that they actually want to look at it, and if it isn't, then you shouldn't be sending it anyway.

Adrian Bye: When you talked about the first round of checks and you're on the accreditation part, if an email is accredited, would that then bypass a lot of the content checks, or does it still go through the same rigmarole.

Anne Mitchell: It really depends on the spam filter of the ISP to what extent they do dispense with all the other checks. In some cases, it doesn't go through any of the other checks, as soon as they see that your IP

address is listed with us, it goes right to the inbox. In other cases, it's given weight, so that they see that you're listed with us and then they look at all the other things and that's because some ISPs, and certainly, I don't blame them for this, or spam filters will say "well, you know, but what happens if a spammer puts one over Surety Mail, or over on Return Path? What happen if that happens?" Now, the ISPs all know that if that were ever to happen, we would immediately summarily execute the spammer by which I mean we will terminate their services. But that doesn't mean that that wouldn't have already come through, and so, some ISP's are very ultra careful and say, you know we really trust Surety Mail but we're still going to check to make sure that the content doesn't look too spammy. If it does, then we're going to look a little more closely at it and see, and the odds are good that because of the weight they give us, that it will still go to the inbox. But that's why I say it really depends on the ISP or spam filter. They all do it differently. By the end of the day, it still means that you're going to go to the inbox or because no one can guarantee that a 100% of you email will always go to the inbox because the ISP and spam filters change their algorithms daily, sometimes hourly. So, it means, it's either, if you're accredited with us, your email will go to the inbox or if for some reason, it doesn't were going to bat for you to rectify that and make sure it does then go to the inbox.

Adrian Bye: How about if someone wants to sign up with your service, how might they do that? How much is the cost?

Anne Mitchell: We have many free resources at the site as well, so you can go to Suretymail.com. Although, you so kindly said ISIPP so many times, that it may have been ingrained in their heads. They can also go to ISIPP.com and all roads will lead to Rome there, and again, we have many free things, free resources there for you whether you sign up with us for accreditation or not, but you can certainly find out there for email accreditation and the cost will depend on your business model we actually have a unique pricing structure because we want to make sure that everyone could afford this, and so, rather than basing the pricing on volume, for example, which other places may do, it really depends on your business model is, and that way, it's affordable for everybody.

Adrian Bye: Okay, Anne, thank you very much for your time.

Anne Mitchell: Thank you. Thank you ever so much, it's always a pleasure, Adrian.