ICANN Transcription
ICANN Whois Privacy/Proxy Abuse Study Findings Webinar
15 October 2013 12:00 UTC

Mary Wong: Hello, this is Mary Wong again from ICANN. Just to welcome all our speakers and participants to today's Webinar. Greetings to David and Tony who have joined the team on the presentation. We will just wait another minute or so for a few other participants to join either through audio Adobe Connect. We do have a number of people signed up for this morning or this afternoon's session depending on where you are. So we'll just wait a minute or so. Thank you.

Hello again, this is Mary Wong from ICANN. And once again to welcome everybody to today's Webinar. We have a number of people in the Adobe Connect room and on the audio bridge and we do have a number of ground rules and standards that I will ask my colleague, Nathalie, to remind us all about. Nathalie, over to you.

Nathalie Peregrine: Thank you very much, Mary. This is Nathalie from staff. Just to remind you all that there is audio streaming in the Adobe Connect room and this means that you will be able to hear the presentation and follow what is happening on the Chat.

However at the end of this presentation if you're also connected on the audio bridge you'll be able to ask questions. There will be a question and answer session after the presentation at which point the operator will open your lines in order for you to be able to ask questions directly.

If you do not wish to join the audio bridge that is not a problem, you can always type your question in the Adobe Connect Chat hub, if you would just like to write 'Question' before it so we can isolate the questions during the presentation and that should be fine.

Equally if you have any technical difficulties during the presentation please don't hesitate to write it in the Chat and we'll be happy to assist.

Thank you very much, Mary, over to you.

Mary Wong: Thank you, Nathalie. And once more, good morning, good afternoon, good evening to everybody. I'd like to extend a welcome to all of you on behalf of ICANN and in particular to Dr. Richard Clayton and his colleagues from NPL who conducted this study on Whois privacy and proxy abuse for ICANN.

Just a quick introduction before I had it over to Richard as his team, as many of you know ICANN has been doing a number of studies on the - on various aspects of the Whois system and this particular study is one of them.

A number of them focused on, for example, relay and reveal requirements and feasibility, the validity of Whois details that was done by NORC from the University of Chicago a while ago. And at the moment we are waiting a completion of a study by Carnegie Mellon University on Whois misuse.

There are more precise details, as you can see, on the link on the slide. And we will provide these slides as part of the recording after this Webinar. So with that introduction I'd like to hand things over to Richard who will take us through NPL's methodology and findings as part of this privacy and proxy abuse study. Richard.

Richard Clayton: Hello everybody. This study is not just me, it's a whole team of people. Tyler Moore and Southern Methodist provided us with data on typo-squatting, which is one of his specialist areas of research and provided us with introductions to some of the other people who provided us with data.

Dr. Nicholas Christin from Carnegie Mellon, one of his specialist research areas is on information about unlicensed pharmacies. And I was assisted by colleagues at NPL, Dr. Tony Mansfield, who did a lot of the experimental design and a lot of the statistics and David Hindley who did all the project management and tried to keep us on track.

The contract for this started - was finally awarded to us in April 2012. We issued a draft report a few weeks back and there's currently a public comment period running on that report, which ends on the 22nd of October.

Now just to get everybody on the same page here and the jargon, as we all know when people register domain names then the registrant supplies their name and contact details for themselves and there are also other fields where you may give details of an administrator or billing contact, a technical contact, a zone contact maybe, and so forth.

And sometimes when the registrant is the same as one of the other contacts then even if you don't get a phone number in the registrant field then you can learn their phone number, well and other details of their - email and so forth, from the other fields. Now all this data is public and is available on the Port 43 Whois service.

Now there are two sorts of ways in which people can fail to supply this information by using privacy and proxy services. And we use a very precise definition here as to what we mean by the difference between these two.

A privacy service is where the registrant's name is provided and is made public but the contact details, which are provided, are essentially generic and they are the contact details provided for all users of the privacy service.

Now sometimes there is a specific per domain email address which is provided to allow so that email can be automatically forwarded but it's still basically the details are generic.

A proxy service is the same as a privacy service except that the registrant's name is not provided. Again, there may be a domain-specific email address but essentially all the details here are generic.

Now what ICANN originally asked people to tender to do the work for was to assess the truth of a hypothesis, which they set out, which was that a significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered by a privacy or proxy services to obscure the perpetrator's identity.

Now when we looked at this we thought well that's all very well but we thought it would also be useful to consider whether or not I'll note another hypothesis which is whether or not when people use privacy or proxy services to register domain names which they use for illegal or harmful activities whether or not this increases the percentage of usage of those services compared with the equivalent percentage of domain names which are used for entirely lawful activities.

I.e. the first hypothesis says, "Are people doing bad things? Are the domains registered using privacy or proxy services at all?" And the second hypothesis asks whether or not this is more than usual rather than just at all.

And the third thing we wanted to look at was that since there are other ways of hiding your identity, for example, putting in registration details for Mr. Mickey Mouse Disney or something like that, basically fake details, then we wanted to extend the study in order to assess whether or not there was valid contact information so when people didn't use a privacy and proxy service were they in fact providing valid information?

And in particular we chose to assess the - whether or not this information was correct by taking the phone number, if it was provided, and ringing up the registrant of the domain in order to ask them - in order to see whether or not we could get a hold of them and whether or not, when we asked them, they were prepared to say yes to the simple question, "Did you register this domain?"

Now just to act as a spoiler here, this is what we found from our study which is, yes, people who register domains, which are used in illegal or harmful activity, they do use privacy and proxy services.

And the second hypothesis, which is that they're using privacy and proxy services more than people who are doing lawful and harmless activities, that's sometimes true but it's sometimes not true as well so it's only partly correct.

And when we look at whether or not we can get a hold of people who have registered domains we find that many domain name registrants don't provide working phone numbers in all cases. But when we look at the usage of - the - try again - when we look at the illegal or harmful ones then we find that it is quite uncommon that we can actually get a hold of the registrant. There's quite a distinct difference here. And we'll go through and show the numbers for upholding what I've just said there.

So first of all let's summarize what we did. Our basic approach was we got lists of URLs from various places and in some cases from experts in the field, some cases from people who publish lists for the use of people blocking bad things and so forth.

We then took all of those URLs and we picked out the domain names. We were only studying Biz, Com, Info, Net and Org. I say only but of course that covers a high percentage of all of the domains which are registered at all.

And then we looked at the Whois data and we used our expertise to assess whether or not there was a usage there of a privacy or proxy service. It sounds very easy but there are a number of edge cases which you need to get right.

And if the registrant details were available, i.e., they weren't using a privacy or proxy service, then we determine what the contact phone number was for the registrant using the information in the Whois; not using any other information, we didn't look at the Websites or anything like that, we just took the information from Whois.

And we then recorded the data for what we find and of course because we're doing accurate counting here then we're getting very precise statistics for privacy and proxy usage and the cases where there is no phone number at all.

However, we didn't have the budget to ring up all of the very large number of domains we looked at which is somewhere over 70,000 or so so we didn't have the budget to ring up everybody so we sampled - we took a random sample from the - from the domain names which had no phone number and then we made a phone call, or at least our subcontractor did, and that phone call was made at a suitable time of day given what country they appeared to be in.

And then in the registrant's apparent native language, so if they appeared to be in China we rang them up and the question was asked them in Chinese. And the simple one-question survey we asked them was: Did you register Example.com, for the appropriate value of the domain which we were ringing up about.

There's full details of all of this and the call schedules that we used in order to maximize our chances of getting hold of people depending whether or not we thought they were businesses or individuals, all of that's in the report in excruciating detail.

Now when we actually rang the people up we got a series - or attempted to ring the people up - then we got a series of different results which it's important to understand how we classified these.

Now first of all in order for a phone number to count towards our random sample that we were going to attempt to ring up then the number what we call apparently valid which means that it looked like a phone number so it had to be long enough and have enough digits.

We excluded all 9s or all zeroes because we felt that these were not phone numbers but people filling in Web forms trying to make the Web form stop complaining that they hadn't filled in all the fields. And we also, for North America, we checked whether or not the area code was valid.

That's rather more difficult to do in other parts of the world but in particular in North America lots of people know about 555 as an area code because they watch the movies and in Hollywood and they, and quite a number of people, use a 555 number in order to indicate that this is not a valid phone number and we treated that as being not valid.

If we did - if the number was apparently valid, then we tried to make a phone call to it. But of course when we tried to make a phone call the it may be that the number wasn't valid and therefore we got an automated message from the phone system which said, no, this is not a valid number or it's too short or whatever. And therefore that counts as invalid.

The next possibility was the number was valid and connected to something but it just rang and rang and rang and nobody ever answered it. Alternatively we might reach voicemail or we might have somebody pick up the phone and we said please can we talk to Mr. Smith, because Mr. Smith is the registrant of this domain name, and either they couldn't help us reach Mr. Smith, they said we've no idea where he is today, or he's in a meeting and he can't speak to you.

The other - next possibility was that the phone was answered and we said could we speak to Mr. Smith? And they said we have never heard of Mr. Smith. And so we said, but he registered Example.com. And they said, no, we've never heard of that either. And so clearly what's happened there is that somebody's details have been stolen and used without their permission.

Or alternatively of course we rang up Mr. Smith and talked to him and said did you register Example.com? He said yes of course I did, thank you very much.

So those are the basic situations. And we split those up. We deemed them as if there wasn't a phone number which was apparently valid we treated it just the same as if there was no phone number at all. If the number failed, as in we dialed this and the phone system said, no this doesn't connect, then we treat that as a failure.

And if we ring it up and the people deny they've ever heard of Mr. Smith and never heard of the domain then that's a failure as well. Clearly if we talked to people then it's a success. If they say, yes, we registered this.

And then we have these categories in the middle which are neither a success nor a failure. And we treat them as being neither a success nor a failure because if we'd rung them up and said, convincingly of course, hi, you've just won the national lottery and you have £1 million coming to you. Once they stop treating this as a scam then maybe they would have said, yes, we'll drag Mr. Smith out of a meeting for that.

So for these ones because we're not sure whether or not it's just the fact we were doing a survey about domain names and we couldn't reach Mr. Smith then we're not really sure whether or not those are successful failures so we leave them in this undecided category.

So let's look at the first work package that we did because the actual thing we did we split up into nine different work packages looking at all sorts of different types of activity.

And the first work package we looked at was phishing which is, in our definition, the creation of fake Websites to steal security credentials. One usually thinks of this as fake bank sites but also you'll get fake sites for email services, for online games and so on and so forth.

And we had, from various feeds that we get all the details in the report of course. From the source data we got we've got - we had some 32,000 different URLs in a week. And when we crunched this down we ended up with 5000 domains of which just over half were in the Biz, Com, Info, Net, Org that we were looking at.

And we then used specialist knowledge to split these into three groups because phishing is not just one sort of activity. Some people set up phishing Websites by maliciously registering domain names. And there were 449 of those.

Some people just use free Web hosting or they use URL forwarding or something like that and therefore those domains are registered by third parties who are basically setting up infrastructure for everybody to use. And it just happens in this case it's used by the bad people who are doing phishing.

So when those domains were registered they had no thought of hiding themselves over and above any thought they had in the first place when setting up the domain.

And the third category, and people often think this is the main category of phishing and our data shows that was the biggest category that particular week, is Websites which have been broken into and then extra pages added in order to do phishing.

And clearly here the domain name has been registered by some individual or business in order to run - to have their Web presence. And the choice as to what they were going to do when they set up whether or not they were going to use a privacy or proxy service, whether or not they were going to provide a valid phone number was made independently of the fact that one day their site was going to be broken into and used for phishing.

So when we look at the data here we find that the privacy and proxy usage on the compromised machines is 24.7% which is pretty consistently - it's higher than the figure that NORC got from their study, which was about 20%, but not a huge amount higher. The maliciously registered domains were distinctly higher at 31%. And the third parties were distinctly lower at 13.7%.

When we tried to ring the people up then the third parties we could ring up about 1/3 of them, the compromised machines we could ring up about 1/4 of them and the maliciously registered domains we could actually ring up less than 1 in 50 of them, i.e. almost none of them.

If we collate the data in a slightly different way, which we think is much, much more helpful way of looking at this, if we asked a priory before we actually did anything at all when we look at the Whois data and based on our statistical knowledge of this particular area then do we have no hope at all of making a phone call to the registrant of the domain?

And in the case of third parties about half the time, 49.6 of the time, we have no hope at all of ringing up the person who registered the domain because - and that 49.6% is made up partly from usage of privacy and proxy services and partly from failure to provide a phone number or not providing an apparently valid phone number.

For the compromised machines, which is just basically random small businesses, then it's about - it's just under 62% is of a priory analysis that we - that you have no hope at all of reaching this registrant on the phone. For the maliciously registered domains then you're not hope at all is 92.5%.

And of course the gap between - if you add the 92.5% to the 1.8% that shows you the gap between them is this category I talked about on an earlier slide where you might or might not be able to get a hold of people depending what sort of question you were going to ask or whether or not you were more persistent in dealing with things like phones ringing forever or reaching voicemail.

So when we look at other types of malicious registration we get very much the same pattern. So when we look at data from advanced fee frauds and other sorts of scam-like - well, (unintelligible) covers a range of things, see the report for all the details.

But basically these are all - these are all malicious sites and so forth but we find just under half of the registrants using privacy or proxy services, so way above average there, and nearly 90% impossible to contact by phone.

When we look at unlicensed pharmacies, which we're all familiar with, then, again, a very high proportion of people using privacy or proxy services but many of these sites do provide Whois information but they don't provide a phone number or that phone number cannot be expected to work.

When we looked at child sexual abuse image Websites, well, sorry, we didn't look at them, when we looked at the data for about child sexual abuse image Websites, then we found only just under 30% of registrants were using privacy or proxy services.

Now for this particular category we didn't make any phone calls at all partly because we didn't think people would be honest when we said did you register this domain, and partly because a lot of our data was most of a year old because we used a whole year's worth of data to get a reasonable sample size. So we didn't ring these people up.

But what we were told by the experts in this area is that their belief is that none of the Whois data is ever valid at all, 100% are impossible to contact by phone.

So what we're seeing here is different rates of usage of privacy or proxy services depending on what type of malicious activity is going on but a pretty consistent story that 9 out of 10 of them you have no chance at all of making a phone call to.

We also looked at some legal and harmless categories so we looked at some legal pharmacies which we got from the legit script list. We looked at an international association of associated law firms. We looked at executive search consultants or headhunters, if you prefer.

We looked at banks, in fact. And we looked at sites from the Alex Top 3500, though in fact we looked at the ones which were being a typo-squatted. And I'm going to have some more to say about typo-squatting later on. But these were the original sites so this is Amazon.com not Amazon.com with two Zeds, that's - with two Zeds it's a typo-squatter, with one Zed it's the real thing. And we looked at whether or not that sort of site were using privacy and proxy services and so forth.

And we also looked at adult - again, we didn't look at, we looked at the data for - adult Websites, i.e. perfectly legal Websites carrying pornography of various types, in order to see whether or not they are using privacy or proxy services and whether or not we were able to ring them up.

And the first column on the slide shows the usage of privacy and proxy services which you see varies from 8.8% for the legal pharmacies all the way up to 44.2% for the adult Websites. And you'll see that in a number of these cases we're getting numbers which are higher - comparable with or higher than some of the malicious and unlawful activities we were talking about earlier.

If we look at the last column, which is did we manage to reach them by phone, then we have the various data there. Now there's a caveat on this because in some cases these were fairly small samples and therefore there are quite big error bounds on those so this is not a very helpful column to look at if you want really robust results.

But the impossible to reach figure is robust and has very small error bounds and there you can see that the figures range from around about 1/4 all the way up to around about 1/2 depending on the particular category.

So the story so far is that the average usage of privacy and proxy services, according to NORC, who measured across all possible domains, is 20%. Our most average set is probably the compromised Websites on the phishing set where it's about 25% so comparable.

Privacy and proxy services are used more often than average for maliciously registered domains. This is universally true but there's a huge range here from just under 30% all the way up to nearly 55%. But some of the legal and harmless activities are significantly - statistically significantly above average as well; banks, 28%; adult Websites, 44%.

But if the privacy and proxy services are not being used then there are other ways of - that the people maliciously registering domains are using and in particular when we look at the phone number, which is all we (did) the data on, then we're getting a range for malicious registrations somewhere around

90%, sometimes 100% whereas the legal and harmless is distinctly below this.

So we also looked at a couple of other data sets which are a bit more complicated to understand. In Work Package 8 we looked at domains from StopBadware which is basically domains where malware may be present. Now these are mainly compromised sites but there are some malicious registrations in this list as well.

Here we found 24. - 20.4% using privacy or proxy services, so pretty average, and 51% not possible to reach by phone so basically this is more like the not maliciously registered sites in terms of the results we're getting.

SURBL, which publish a list of domains which indicate that email may be spammy, i.e. this is probably not email that you want to accept and put into an inbox. Most of these domains are maliciously registered but it's not universally so. There we found 44% using privacy or proxy services but only 58.5% not possible to reach by phone.

Now there are some cautions about the SURBL data because we found that many of the domains have the same contact phone number, i.e. they were all linked together.

And they've probably been put onto the list by SURBL because of links between them and this causes various statistical effects which means that a - basically how a small number of people behave affects the overall results of the work package and that means that we get higher abounds and therefore there's a number of notes of caution about how you interpret the results for WP8.

Now I've already mentioned domains like Amazon.com, which sometimes are type escorted i.e., small variations of the main names are registered. And people hope to monetize this because if people misspell amazon.com as they're typing it in then they hope to show the mappers make money.

The type of squatting domains which we looked at then we found quite a high usage of privacy and proxy services -- 48.2 -- one of the highest figures we saw.

But we found that 10.6 were reachable by phone but which is a higher proportion than adult Web sites. But there's some quite high error bounds on these figures.

And similarly Web package nine we looked at domains which had been subject to the UDRP again just from the standard set of these com net info and org. And here we're seeing our privacy and proxy services used by just under 40% of registrants.

Now what we - the way we interpret this data is the type of squatters are coming to groups, some of them are trying very hard not to be identified whereas others don't care.

One possible explanation for why this happens is the type of squatting is not necessarily criminal and so you're not being chased by the police.

But if you do cybersquatting at scale then a brand owner may be attempted - more tempted to come after you than if you appear that if it's not clear that all of those domains type of squatting of brand are owned by the same person.

A slide here on the statistical significance here, basically, as I mentioned right at the beginning because we did exact counts all the way through, then and since for many of the work packages we have very large samples -- tens of thousands of them in some cases -- then we expect that our results are pretty robust.

Albeit we did sample for particular weeks or months and things change over time but not all that fast.

Most of the variations between our figures for privacy and proxy services and so forth which are greater than the 3% difference then they're statistically significant at 90% or better again all the details in the report.

The phone calls to registrants we sampled and we did a random sample from the domains. But we avoided calling the same number more than once, so that we didn't get people board so that they lied to us because we were ringing them up several times.

And see the report for the rather contract statistical analysis which is needed in order to reflect the way in which we did this.

There are some cautions about the error bounds because of the small sample sizes, and as I already mentioned these large groups of domains owned by a single people and that causes some difficulties.

But what I would assure you is that the analysis of it's impossible at (Peoria) we believe to make a phone call to this registrant at very much lower error bounds.

And that's the most robust indicator that we have. And, in particular, it shows that the malicious registrants are choosing a range of different methods of being contactable not just choosing between privacy and proxy services.

There is a slide here which I'm not going to go through it all here which basically summarizes the numerical results of the study.

And we now get on to the overall conclusions which is what I've been saying all the way through, which is when, we're - when domains are maliciously registered then privacy or proxy services are used more than average -- no question about that.

But there are some legal and harmless activities that are also using privacy are proxy services significantly more than average.

And when privacy and proxy services are not used when a domain has been registered for malicious reason then the valid ballot phone numbers are pretty rare so that the overall effect is that at least nine out of ten of registrants can't be reached by phone.

But it's also true that for many lawful and harmless activities the Whois details don't contain valid contact numbers either with anything between 1/4 and 2/3 depending on this (whole track) awful and harmless activity we're talking about, they are unreachable as well.

But of course if you're trying to get a hold of some legitimate business then you may have more clues to go on than just of the phone number in the Whois as a way of reaching.

So that's all I want to say about the report. There's a link here to the public comment page, and so forth. And written public comments are extremely welcome.

The deadline is midnight UTC on the 22 of October. But please the whole point of asking for comments is we're asking for comments on the report and not on what you think of the Whois system altogether.

We're interested in whether or not we've made any errors in our methodology. We're interested in whether or not you think we have misinterpreted what we've seen or whatever.

So please don't give us long assays on what a he wicked thing criminality is or what difficulties you had in dealing with some particular domain. That's not what it's for. The comments are meant to be on the report.

So now we're going to do a Q&A. And I'm asked to remind you that if you want to talk to us in order to do that, then you can't do it through the Adobe Connect Room. You need to dial in to the bridge.

Mary Wong: Yes, thank you very much, Richard and the MPL Team for a very comprehensive study and for a very clear presentation of the results.

As Richard has said we would very much welcome public comments on the methodology and findings of the report as it'll be very helpful indeed to the team and to ICANN in further refining the study as well as its impact on the Whois system generally.

If you have a question for Richard or anybody on the team please feel free to ask. Olivier I see that you raised your hand. Please proceed.

Olivier Crepin-Leblond: Thank you very much. Mary. It's Olivier Crepin-Leblond for the transcript record. Can you hear me?

Richard Clayton: Yes, indeed.

Mary Wong: Yes.

Olivier Crepin-Leblond: Okay fantastic. Thank you. I just have a question just summarizing the results. First, well done for this study. I think it's very much welcomed by our community.

But also it certainly points out that there is a significant amount of crime going on with regards to these privacy services and not only privacy services but with regards to inaccurate Whois records.

So the question that I have really to summarize it all I do understand that there is a significant amount of privacy services used for legitimate reasons.

Do you have a percentage - and now I might have just missed it in the presentation here, but do you have a percentage of how much of Whois services, privacy services are used for legitimate reasons, and how much of it are used for illegitimate reasons?

Richard Clayton: I don't think we can really say that because what we don't know - what we know is that overall the usage of privacy and proxy services by domains as a whole on the (Nork) sampling study is 20%.

The nearest figure we have to compare with that is the figure from the compromised Web sites which is essentially measuring small and medium-sized Web sites where they don't have specialty security teams so they get broken into and used for fishing. And there the figure was around about 25%.

But since we don't know how many maliciously registered domains there on total it's rather difficult to subtract those off from the 100 million or whatever total domains in order to say whether or not that figure, the 20% is being biased upwards or biased downwards in fact from the various producers activities going on.

In general I suppose one has to say it's been moved upwards, but equally an awful lot of domains are parked at any given point. And there - they - those tend to not to be done using privacy and proxy service and that again distorts the figure.

So overall I would say that for at some random domain which you didn't think was malicious then 20% to 25% chance use it for visual proxy services.

But in some specific areas, for example, adult Web sites then it's from our measurements 44%. So clearly other people who run - who own pornographic Web sites don't want their mom to know that they own them.

But equally, if we look at banks and in general people who are bankers are proud to be bankers there we're seeing almost as the same percentage of usage of privacy and proxy services as we're seeing on child sex abuse image Web sites.

So it's a complete mixture of results here. And it's very hard to give an overall figure here are or an overall impression because it varies by activity.

Mary Wong: Thank you, Richard. Olivier did you have a follow-up?

Olivier Crepin-Leblond: Yes, thank you Mary. It's Olivier again. And thank you for this explanation.

Whilst you were describing the various studies and work that you were doing somehow I wondered whether you would have any recommendations or thoughts as to what further study might be required.

I've heard here an extensive study on more domains. Are there any other further studies that you would recommend so as to get a clear picture and a more exhaustive picture?

Richard Clayton: I think the thing that the community needs to understand is whether or not the people who use privacy and proxy services are in fact hiding their identity from the privacy and proxy service as well or whether or not in practice it's basically just a shield and they really are just protecting their anonymity.

So that once you understand that and whether or not you can - whether or not if you're law-enforcement or somebody with appropriate legal standing whether or not you can see through the privacy and proxy services then that gives you a better idea as to what sort of damage they might be doing.

Mary Wong: Thank you. Thank you for those questions Olivier and thank you for the answers, Richard. There might also be some people on the audio glitch, but not in the Adobe Connect who may wish to ask questions. If you do, please go ahead and speak.

Richard there is a question that has been posted to the Adobe Connect chat room.

Richard Clayton: Yes I can see that. It has been asked by (Carlton)...

Mary Wong: Yes.

Richard Clayton: ...who asks - who says did the study show privacy and proxy services used unreachable phone numbers?

And the answer to that is that we didn't actually study that. We didn't make any calls at all to privacy and proxy services.

Actually, that's not quite true. We made - I think we made one by mistake as a categorization error at an early stage of the study. But we didn't actually examine that at all.

In general my experience of looking at privacy and proxy service Web sites and so forth is that they're much more interested in having you reach them through email or through Web forms rather than bringing them up.

So there are - there's a limitation here in that we're using phone numbers overall as an indicator of reachability whereas that may in fact not be quite completely reflect the real world situation here as to help people wish to be contacted.

We didn't use email because we thought that if we sent out a survey question by email apart from being accused of spamming by everybody in sight by sending out lots and lots of questionnaires, we wouldn't expect to get a particularly high response rate.

Whereas if you bring up people and put them on the spot and you're - and you really are just asking one question there's a reasonably good chance that they would answer you and that in fact the results we got from the survey showed that very few people actually refused to talk to the people during the survey.

We got response when we did reach people. We got coherent responses very quickly.

Scott Austin: Excuse me, I have a question.

Mary Wong: Yes, please go ahead.

Scott Austin: Yes, hi. This is Scott Austin. I just had a question about when the study was created. Was there a policy directive that it was identified as being useful toward?

Is there something on the table currently that would change the way that this data is provided? For example, there would be some kind of identification or proof such as a passport or driver's license or something that's tied to the registrant?

Richard Clayton: I can't answer that. Mary might be prepared to comment.

Mary Wong: Thanks Richard and thank you Scott for the question. I should of said at the beginning that not only is this particular study part of a series of studies that ICANN had commissioned on various aspects of the Whois system but that the terms of reference for this and all the other studies were developed in large part through public comments that were received from the community at the time.

So one of the things that we are hoping that the comments for this and other studies might reveal is aspects that could be done as follow-ups, either because of things revealed by the results or because of questions that the community believes we ought also to ask, but in particular at this particular time.

And it may well be for those familiar with the ICANN community and system that those may or may not be done to further studies or perhaps through a for policy development process within ICANN itself.

So I can't answer your specific questions because I don't have all the prior background in front of me.

But if it is an issue or a question that the community believes would require further study then, first of all I hope that that will come through in the public comments.

And secondly I can let you know of that the ICANN will certainly take that under consideration very seriously.

Scott Austin: Okay thank you very much.

Mary Wong: I see that there is another question in the Adobe Connect chat room from (Orrin D). And your question I assume is to ICANN staff.

What are the action items from this study? Clearly, there is a problem that has been known for years. And thank you for the compliment to the researchers on the study.

And your comment there is that this great study just proves that there is a problem.

(Orrin) I think that this goes back to the response I gave to Scott just prior to this, which is that if there are specific questions or issues that the community believes we ought to do either further studies on or start a policy development process or PDP on please let us know.

We can't and we won't act without the input of the community. And perhaps these may be areas that require further study and follow-up from here on out.

(Lisa) I believe that you raised your hand?

(Lisa): Yes I just wanted to add a perspective. I was involved in the definition of the terms of reference that led to this study and some of the others.

And some of the questions that we were hoping to gain insight into from this study were for example if there are particular kinds of malicious activity that were more prone to using privacy and proxy service were to the point that Richard is made quite a few times in his presentation, how to compare the rate of use of privacy and proxy service by what he calls malicious registrants to the rate of other ways to obscure contact information or identity information, such as providing inaccurate Whois.

And I think that the goal of this study was to help us as we go forward with the policy development process to understand the relative significance of those two kinds of activities as well as malicious - excuse me, another activity that Richard highlighted briefly which was the use of compromised Web sites as the launch point for malicious activity.

So this gives us a way to focus on where the real problems lie rather than assuming that all of these different kinds of ways of obscuring the identity or contact information for malicious registrants assuming that they're all equal and all bare the same amount of scrutiny or policy change.

Mary Wong: Thank you (Lisa). And just to follow-up on that this is Mary Wong again that we really at ICANN do hope that these studies and findings do show us greater clarity as (Lisa) has mentioned.

I see on the chat that there is a statement from (Carlton) that the At-large Advisory Committee, which is as you all know, one of the advisory committee to ICANN has put on record that privacy and proxy services must be regulated.

I should note for everyone attending for the record that ICANN has already committed to developing a privacy and proxy service accreditation program.

And again to that end, we believe that this study and these findings will be very helpful. And there's also other activities in other parts of the ICANN community, for example, a policy development process that's ongoing in the generic names supporting organization to look at certain specific issues relating to privacy and proxy service accreditation.

And I see from the chat that Olivier as (Carlton) points out as the chair of the ALAC has posted a link to the statement that is currently being voted on by the ALAC to be submitted to ICANN I assume on this and a another number of other issues as well. So thank you all for that.

And I was wondering Richard while we wait for perhaps a couple of other questions do you have any comments or thoughts on patterns of privacy or proxy usage that were somewhat surprising as you surveyed the results of the study?

Richard Clayton: Well one of the interesting things I noticed was that in general privacy services are extremely uncommon at that most people use proxy services instead.

About the only exception was the banks. And the reason that their figures are so high is quite a number of them have used a particular registrar and that registrar offers a - doesn't offer a proxy service but does offer a privacy service. And they've chosen to use that.

The interpretation I put on this is that if you are some somebody technical in a bank and you're wishing to register the bank's domain name that it does occur to you that you don't want people ringing you up all of the time, saying that the bank Web site has crashed and what are you going to do about it because all you're doing is registering a domain name and being the point of contact for that domain name.

Whereas that would be not an appropriate route into the bank for dealing with the Web site is crashed or my money has come from my account or whatever.

So I think that there are reasons why people choose to use, privacy and proxy services which go beyond anonymity as we usually think of it into I didn't know we should be contacted about this. There are better ways of getting a hold of my company.

Mary Wong: Thank you. And that is kind of an interesting observation.

I should note too that, as you mentioned that there is a nuance and perhaps a distinction too in the usage of privacy versus proxy services.

And that's one reason why the team I think in one of its very first slides put up the working definition that we used for both services in this study.

And I would point everyone to the study itself because many of the details, including what Richard has just spoken to are explained in further detail in that study.

Are there other questions, either in the Adobe room door on the audio bridge for Richard or the team or ICANN?

Scott Austin: Yes, this is Scott Austin again. One other question regarding the qualifications for proxy and privacy services, I guess are there - because of the comment about regulation in the chat room, how difficult is it to own one of these?

And is it possible that some of the very people that we're concerned about with malicious sites actually run a known proxy your privacy services?

Richard Clayton: I have no idea who runs privacy or proxy services. They basically split up into a number of groups in that there are people running privacy and proxy services who sell this as an add-on to a whole range of registrars.

There are then privacy and proxy services which are registrar specific so that you will only see that privacy or proxy service being used by one particular registrar or a group of registrars because some - in some cases registrars come in little groups and they just have the brand names for the way in which they sell their services to the market.

And then you have various other things which we treated as being privacy or proxy services where clearly our people are registering domains on behalf of customers and then are using their names in the contact details and where is extended to hundreds or thousands of domains then we treated that as being a privacy or proxy service.

And it's arguable. I suppose that these are not privacy and proxy services and that we've overestimated a little bit here. It doesn't make a huge difference the numbers in my view.

But there are a handful of people, not really singling them out especially for any bad reason or whatever.

But blue host.com, for example, has quite a large number of people are buying hosting services off them. And when you look at the contact details on the domains it all says bluehost.com.

And we treated that is being a proxy service whereas it's not really quite the same as the operation run out of (novibeach). And it's not quite the same as, say, network solutions privacy service.

Scott Austin: Thank you Richard and thank you for an excellent study.

Then I guess my question then should go really to the ICANN representatives if there is any vetting of someone who calls themselves a proxy service.

Mary Wong: Scott, thanks for the question. This is Mary Wong for ICANN.

I believe that at the moment there is not. And the reason for that is that at the moment there is no regulation to use the word accounting has used in a broad sense or more specifically accreditation or vetting if you like of privacy and proxy service providers.

As you and Richard have noted, there can be quite a wide range of those who can be considered providers of such services. That certainly should be one thing that we will be looking at.

As I mentioned earlier, we've committed to developing an accreditation service for these providers. And it is hoped that those are some of the details that will emerge that will be informative and helpful to the community, both in terms of looking at rates of usage as well as in determining whether, when and how to use these service providers going forward.

Scott Austin: Thank you.

I'm conscious of the time. We're coming to the end of our hour. I see however that (Carlton) has asked a question Richard in the chat if you'd like to respond briefly.

Richard Clayton: Yes, the answer to which is see slide 3 is that (Carlton)'s asking what's the difference between a privacy out proxy service?

And the difference is that a proxy service, all of the details are generic whereas for a privacy service we learn the name of the person who has registered the domain or at least what they claim to be the domain.

But we don't learn anything about their contact details, their land address, their phone number, et cetera.

Mary Wong: Thank you Richard. And (Lisa) has provided a follow-up in the Adobe chat as well concerning Richard's response.

((Crosstalk))

Richard Clayton: Yes. Sorry - well, what I've done is I've blurred over an important distinction which ICANN is very keen as I make. And if you read the report, you'll see it's made very carefully which is that in a proxy service the strict position from ICANN's point of view is that the registrant is the proxy service, and that somebody else has beneficial usage of the domain. And we get that right in the report.

Mary Wong: Thank you Richard. And as you mentioned, this is very clear in the report. And once again I'll encourage everyone to look at the report and submit a public comment.

I should also mention that on the page that Richard links to in this final slide there are some details as to the background.

This may be relevant to some of the questions asked earlier, including how the terms of reference for this report were developed, as well as a link to another page on the ICANN Web site that gives you background to the other studies as well as some of the recent and ongoing developments relating to ICANN's development of a privacy and proxy service accreditation program.

So we have exceeded by one minute the one hour allocated for this call.

I'd like to thank everyone for participating and certainly Richard for an excellent presentation.

Before we close the recording Richard do you have any final closing comments?

Richard Clayton: No. I would just encourage you to read the report and also admire the help that I got from all the other people, particularly on the statistics.

Mary Wong: Thank you. And thank you once more for a great report. Thank you everybody.

And with that we will close the recording in the Adobe Connect room and we look forward to your comments and feedback on the report. Thank you.

END