Brendler, Beau Brenbe at consumer.org
Tue Apr 28 10:25:10 EDT 2009

* Previous message: [At-Large] Draft IRT report
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

Greetings. As you know I am on the registration abuse policy working group. Yesterday's teleconference was the first I have been able to attend. I wanted to pass on to you the working definition established for abuse and see if anyone has any comment. Please let me know if you do, and I will pass on to the WG.

Beau Brendler
---

Abuse is an action that:

1. Causes actual and substantial harm, or is a material predicate of such harm, and

2. Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.

Notes:

* This is a working definition as per group consensus on April 27, 2009 and may be re-visited should the WG find it inadequate after examining some specific examples.

* The party or parties harmed, and the substance or severity of the abuse, should be identified and discussed in relation to a specific proposed abuse.

* The term "harm" is not intended to shield a party from fair market competition.

* The above definition of abuse is indebted to the definition of "misuse" in the document "Working Definitions for Key Terms that May be Used in Future WHOIS Studies" prepared by the GNSO Drafting Team [18 February 2009, at http://gnso.icann.org/issues/whois/whois-working-definitions-study-terms-18feb09.pdf].

please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

---

Derek Smythe derek at aa419.org
Tue Apr 28 17:22:01 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] ALAC Review Final Comments from the ALAC
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Brendler, Beau wrote:
>.... an action that:
>
> 1. Causes actual and substantial harm, or is a material predicate of such harm, and
>
> 2. Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.
>

It is extremely easy trying to shoot Beau down on phrases such as illegal/illegitimate/predicate without delivering any positive contribution.

I thank Beau for this initiative. It is long overdue.

However those that work with internet abuse on a daily basis, will exactly know what Beau is describing.

As such I will try my hand: Any action that deliberately intends to deceive with the intent of harming, either physically, emotionally or financially, another party on the net.

I am deliberately saying "intends", since this should be aimed at preventing criminals and fraudsters. The golden rule of the net: when the money is gone, it's gone.

Thinking Back, Garth and Jart has a nice definition as well.

Example: annanemmanuel.com - sculptor "Annan Emmanuel"

Any queries on this domain may be couriered via

http://royaldiplomatic.annanemmanuel.com/ or
http://magnatecourier.annanemmanuel.com/ to the legitimate owner of
the content at http://www.sculptorcarver.com/ (though the fees may be
steep and no guarantees it will ever be delivered)

Jokes aside. Where does the legal jurisdiction for the above lie? The
point is the registrant is deliberately hiding. Do we unwrap a trail
of Privacy abuse, only to find fake registration details, then decide
to act with a trail of victims later, or do we see this for what it is.

Another example:

As far as I know, botnets are not illegal in some parts of the world.
Heck, I think LE in those areas may not even know what they are.
However does that make it right for them to attack other parties in
other parts of the world, using botnets in yet another jurisdiction(s)
just because they have no law against it? Or maybe have? Obviously
not. So what are we going to call it?

As such, please understand what Beau is describing and rather try and
support his efforts and help to get this issue pegged down.

Derek Smythe

---

Beau

Thanks for sharing.

The one obvious question that springs mind is the definition of "illegal". Illegal in
which jurisdiction?

Regards

Michele

--
Mr Michele Neylon
Blacknight Solutions

---

Bret Fausett bfausett at internet.law.pro
Tue Apr 28 15:27:20 EDT 2009

* Previous message: [At-Large] Definition of registration abuse

* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

Thanks for this, Beau. A few comments on the definition below, all designed to tighten up the definition so registrants can actually have some idea of what is abusive and what is not.

> Abuse is an action that: 1. Causes actual and substantial harm,

Clarification: to whom? And what kind of harm? Are we focusing on technical disruption? consumer fraud? economic harm to businesses what we are looking? All of the above?

> or is a material predicate of such harm,

This is a hard one, especially when coupled with the nebulous "illegitimate" below. My possession of a lethal weapon is a material predicate to my committing armed robbery, but there's a huge leap between keeping an unloaded rifle locked in my gun cabinet and knocking over the neighborhood liquor store.

> 2. Is illegal

Where? In the country where the registrant lives? registrar? registry? ICANN? For just one example, in the United States, it's not legal for U.S. citizens to run online gambling sites. In some countries, the facilitation of online gambling is the major export.

> or illegitimate, or is otherwise considered contrary to the
> intention and design of a stated legitimate purpose, if such purpose
> is disclosed.

At least "illegal"is capable of definition, by reference to some jurisdiction, but "illegitimate" and "stated legitimate purpose" are not capable of more precise definition than "in the eye of the beholder." I would strongly recommend removing this clause and finding something you can actually define with more precision.

Thanks for keep us posted!

Bret

---

Bill Silverstein icann-list at sorehands.com
Tue Apr 28 15:46:33 EDT 2009

* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

"Bret Fausett" <bfausett at internet.law.pro> wrote:
> Thanks for this, Beau. A few comments on the definition below, all
> designed to tighten up the definition so registrants can actually have
> some idea of what is abusive and what is not.
>
>> Abuse is an action that: 1. Causes actual and substantial harm,
>
> Clarification: to whom? And what kind of harm? Are we focusing on
> technical disruption? consumer fraud? economic harm to businesses what
> we are looking? All of the above?
>
>> or is a material predicate of such harm,
>
> This is a hard one, especially when coupled with the nebulous
> "illegitimate" below. My possession of a lethal weapon is a material
> predicate to my committing armed robbery, but there's a huge leap
> between keeping an unloaded rifle locked in my gun cabinet and
> knocking over the neighborhood liquor store.
>
>> 2. Is illegal
>
> Where? In the country where the registrant lives? registrar? registry?
> ICANN? For just one example, in the United States, it's not legal for
> U.S. citizens to run online gambling sites. In some countries, the
> facilitation of online gambling is the major export.
>
>> or illegitimate, or is otherwise considered contrary to the
>> intention and design of a stated legitimate purpose, if such purpose
>> is disclosed.
>
> At least "illegal"is capable of definition, by reference to some
> jurisdiction, but "illegitimate" and "stated legitimate purpose" are
> not capable of more precise definition than "in the eye of the
> beholder." I would strongly recommend removing this clause and finding
> something you can actually define with more precision.
>
> Thanks for keep us posted!
>

The abuse should include things that has been determined to be abusive, such as front running.

I'd like to think that registrars are in a fiduciary relationship with the public, ie. like a bank or attorney. That if you check the availability of a domain name, the registrar grabs it.

That registrars do not hide the identity of the registrant, unless they accept liability for the use of the domain names.

---

Michele Neylon :: Blacknight michele at blacknight.ie
Tue Apr 28 18:01:55 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


>I'd like to think that registrars are in a fiduciary relationship with the
>public, ie. like a bank or attorney. That if you check the availability of
>a domain name, the registrar grabs it.

I presume you mean "does not grab it"

>That registrars do not hide the identity of the registrant, unless they
>accept liability for the use of the domain names.

You'd need to qualify that.
Most registrars use automated systems to handle the entire process.

If someone registers a domain name to "John Smith" and is actually "Jack Jones" that is hardly the registrar's responsibility.

Now if a registrar was knowingly and intentionally aiding fraudsters to commit fraud then it's a different matter..

Also, private individuals have a right to privacy, which is why registration proxy services are so popular.

If no crime is being committed, then a registrant should have the right to privacy ..

Regards

Michele

---

Bill Silverstein icann-list at sorehands.com
Tue Apr 28 18:12:36 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


>>I'd like to think that registrars are in a fiduciary relationship with
>> the
>>public, ie. like a bank or attorney. That if you check the availability
>> of
>>a domain name, the registrar grabs it.
>
> I presume you mean "does not grab it"
Good question. The problem is that the registrar grabs it, but they should not be grabbing it.

>
>
>>That registrars do not hide the identity of the registrant, unless they
>>accept liability for the use of the domain names.
>
> You'd need to qualify that.
> Most registrars use automated systems to handle the entire process.
So what? These registrar offers domain name privacy services.

>
> If someone registers a domain name to "John Smith" and is actually "Jack
> Jones" that is hardly the registrar's responsibility.
Not until the registrar is notified that the information is not valid. I have seen many occasions where the information is clearly not valid. The reigsrar permits the information to be corrected or gives 15 days to correct the information instead of terminating the domain name immediately.
One example is 123 Yellow Brick Road.
>
> Now if a registrar was knowingly and intentionally aiding fraudsters to
> commit fraud then it's a different matter..
>
> Also, private individuals have a right to privacy, which is why
> registration proxy services are so popular.
>
> If no crime is being committed, then a registrant should have the right to
> privacy ..

Illegal spam is not a crime. Copyright violation is not a crime.

Under the terms of the registration contract, these proxy registration services are liable for harm.

---

Derek Smythe derek at aa419.org
Tue Apr 28 19:41:33 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Bill Silverstein wrote:

>> If someone registers a domain name to "John Smith" and is actually "Jack
>> Jones" that is hardly the registrar's responsibility.
> Not until the registrar is notified that the information is not valid. I
> have seen many occasions where the information is clearly not valid. The
> reigsrar permits the information to be corrected or gives 15 days to
> correct the information instead of terminating the domain name
> immediately.
> One example is 123 Yellow Brick Road.

And if the registrars ignores it trying to make it an issue for courts etc? Here the registrar and ICANN knows the address is fake: http://www.badwhois.info/wp/?m=200902

Some follow up domains have the same fake registration details via the same registrar.

>> Now if a registrar was knowingly and intentionally aiding fraudsters to
>> commit fraud then it's a different matter..
>>
>> Also, private individuals have a right to privacy, which is why
>> registration proxy services are so popular.

Agreed. But "criminals" also love privacy?
Also the same registrar mentioned previously, has privacy policies that even raised a comment in Mexico.

>>

>> If no crime is being committed, then a registrant should have the right to
>> privacy ..
> Illegal spam is not a crime. Copyright violation is not a crime.
>
> Under the terms of the registration contract, these proxy registration
> services are liable for harm.
Will it hold up in court? Maybe, maybe not, regardless of how deserving!

I have personally pointed out fraud being committed (bank spoofs) using private registrations to registrars. The registrars accepted this but allowed much more of the same. In fact this also appears to have become a method of hiding an identity theft problem in registrations where the registrar became aware of the problem.

What about the privacy provider? I recently came across a domain reseller, deliberately in Turkey, claiming privileged relationship with law enforcement that will cause them to turn a blind eye, using privacy providers in Sudan and Hong Kong who also happen to be attorneys. Part of the sell was that they tolerate anything on their services and not law, court orders or similar can get you removed from the net.

Some food for thought:
http://fakewebsitecash.org/

We cannot deny that there is a lot on "abuse" by whichever name on the net, abusing systems, law and whatever to enrich certain elements at the cost of "defrauding" others with fake offers, impersonation etc.

It is just a case of defining this "abuse" as not acceptable, so it cannot be "abused" in itself.

Derek

---

Karl Auerbach karl at cavebear.com
Tue Apr 28 19:46:21 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Bret Fausett wrote:

>> 2. Is illegal
>
> Where?

And to take the next step - there is a tendency in these discussions to jump from a set of
actions to a conclusion that it is unlawful.

Yet in real life legal proceedings there is an intermediary step - a trial - in which the actions are put into context and measured (often quite subjectively) against the rules of law.

It seems to me that in all of these internet matters that one should not jump to the conclusion that something is unlawful until there has been an a concrete legal procedure
that has find that to be the case.

Thus rather than leaping to the conclusion that acts X, Y, and Z are an unlawful abuse of
a trademark and reacting by, for instance, revoking a domain registration it would be
better if that revocation had to be predicated on an actual legal process that concluded
(and had passed through any appeals process) that an unlawful abuse of a trademark had
actually occurred.

Otherwise we seem far too much at risk of inventing a parallel, but different, judicial system.

--karl--

---

Derek Smythe derek at aa419.org
Tue Apr 28 20:20:09 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Karl Auerbach wrote:
> Bret Fausett wrote:
>
>>> 2. Is illegal

>>
>> Where?
>
> And to take the next step - there is a tendency in these discussions to
> jump from a set of actions to a conclusion that it is unlawful.
>
> Yet in real life legal proceedings there is an intermediary step - a
> trial - in which the actions are put into context and measured (often
> quite subjectively) against the rules of law.
>
> It seems to me that in all of these internet matters that one should not
> jump to the conclusion that something is unlawful until there has been
> an a concrete legal procedure that has find that to be the case.
>
> Thus rather than leaping to the conclusion that acts X, Y, and Z are an
> unlawful abuse of a trademark and reacting by, for instance, revoking a
> domain registration it would be better if that revocation had to be
> predicated on an actual legal process that concluded (and had passed
> through any appeals process) that an unlawful abuse of a trademark had
> actually occurred.
>
> Otherwise we seem far too much at risk of inventing a parallel, but
> different, judicial system.
>
>  --karl--
>
>
> _____
> At-Large mailing list
> At-Large at atlarge-lists.icann.org
> http://atlarge-lists.icann.org/mailman/listinfo/at-large_atlarge-lists.icann.org
>
>
> At-Large Official Site: http://atlarge.icann.org
>

How long will this process take?
A good scam takes a day and we have victims, many of which will never be reported to LE, many not understood by the LE reported to. Nobody even knows what the losses are on the fraud on the net! The promise of the Internet is instant delivery. I press a button in Romania and a victim sees the content immediately half way around the world. Legal process is known to be slow. 15 days.

Who will pay for it?
Banks and other legitimate content owners, trademark owners may

initiate take downs on phishing sites since this affects their bottom line directly. As for 419/advance fee fraud sites, not so since their clients are not targeted.

Who needs to initiate it? As we see above, the bank or legitimate owner may not. Yet the targets and victims do exist, else we would not be posting here

LEA? Will the American taxpayer foot the bill for most of domains using American registration details/hosted in the USA? I think that would be unfair. In fact Commissioner Jon Leibowitz asked ICANN way back to improve the whois accuracy. What we see is more of the same and provably so, so what right have we to make it a problem for authorities? How can we expect them to clean up if we are just making it more complex for them, but refuse to clean up house?

Why go through this process if the same registrant is proven to have numerous identities and keeps on repeating this process time and again?

In certain instances the same parties have been at it for up to 5 years, have built mansions, are driving around in the most expensive cars .... safely in countries notorious for scams and a severely lacking justice system. They use American debit cards complete with American address to purchase domains. In fact providers who sell these supply them with access to paid for proxies when they purchase these cards from them. This is just one example. Trying to follow the money trail is near impossible.

Theoretically yes to what you are saying if we talked about an issue in a single country where everybody was law abiding, we had real registration details, where had honest registrars, there we no criminal resellers. However we are not. We are crossing international borders with the average consumer simply being cannon fodder. This is the real world scenario.

The problem is simply that if we do not resolve this, at some stage authorities will get involved and we may lose a lot, not just only privacy. Look at the .US TLD.

Derek

---

Karl Auerbach karl at cavebear.com

Tue Apr 28 20:28:29 EDT 2009

* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

Derek Smythe wrote:
>
> Karl Auerbach wrote:

>> It seems to me that in all of these internet matters that one should
>> not jump to the conclusion that something is unlawful until there has
>> been an a concrete legal procedure that has find that to be the case.

> How long will this process take?

As long as it takes. Otherwise we will have a system in which a mere accusation is sufficient.

We recently saw in New Zealand that the copyright people tried to push through a system in
which people could have rights taken away - like being denied access to the internet - by
the mere accusation that they were violating copyrights.

And have we not learned enough of how things can get bad through "expedited" processes
such as in the DMCA?

Personally, I'd rather have justice than a system that could very easily turn into e-witch
burning.

Inventing a new, fast alternative legal system - which is what is being suggested here -
is something that ought not to be done without the most careful of reflection.

--karl--

---

Derek Smythe derek at aa419.org
Tue Apr 28 22:26:53 EDT 2009

* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse

* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

We are missing a point here.

USA: It is illegal to access/host child pornography. (and rightly so, also where I am)
Rest of the world: see http://www.canadiancrc.com/Newspaper_Articles/InformationWeek_Study_Child_Porn_Isnt_Illegal_Most_Countries_06APR06.aspx

USA: It is okay to look at pornography
Saudi Arabia: illegal

So whose laws? Unfortunately we do not have a global government, laws vary. But we have a global net and domains. Some countries with civil upheaval are abused by internet criminals. Domain privacy lawyers in the Sudan - please!

Show me something one the net and I could either make it illegal or legal, I just jump jurisdictions. This is exactly what criminals rely on. Proxies etc do not help.

Yet the Internet is not a new phenomenon and is in fact developing extremely fast with the convergence of technologies and new technologies. Laws lag, some much more than other places, but especially on the net.

80% of the USA is connected. 80% of the world is not connected.

Yes, I am mentioning extremes because this is the nature of the net.

No, we do not have to railroad this process. However I agree with seeing justice, but we cannot enforce legal cooperation either, that would be a bit like the tail wagging the dog. Each country has it's own priorities. The international aspect of the net does cause problems and we have to accept this. How clean or not we intend keeping the domain sphere will reflect on how much politicians, lawyers and LE gets involved or not. It is in every bodies best interest to keep the house clean.

So why not start of with:
Is phishing okay?
Is spamming okay?
Are 419 scams okay?
Are eBay scams okay?
Are moneymule scams okay?

...

What is not acceptable and why is it not acceptable? What is common, what not? This is exactly what is being attempted. It is not a quick fix, no railroading or witch hunts, but defining what the general consensus is. How was the McColo issue resolved? Estdomains? By lawyers, LE, Policians?

We are not going to ever resolve this with any country's laws. But somewhere we will have to define an accepted norm because we cannot maintain the current status quo.

However I guess we could end up with something like a $5.00 legal fee on each domain registration/renewal for LE purposes if we continue on the current route. That would then leave ample leeway for politicians, attorneys and LE to get involved.

Derek

Karl Auerbach wrote:
> Derek Smythe wrote:
>>
>> Karl Auerbach wrote:
>
>>> It seems to me that in all of these internet matters that one should
>>> not jump to the conclusion that something is unlawful until there has
>>> been an a concrete legal procedure that has find that to be the case.
>
>> How long will this process take?
>
> As long as it takes. Otherwise we will have a system in which a mere
> accusation is sufficient.
>
> We recently saw in New Zealand that the copyright people tried to push
> through a system in which people could have rights taken away - like
> being denied access to the internet - by the mere accusation that they
> were violating copyrights.
>
> And have we not learned enough of how things can get bad through
> "expedited" processes such as in the DMCA?
>
> Personally, I'd rather have justice than a system that could very easily
> turn into e-witch burning.
>
> Inventing a new, fast alternative legal system - which is what is being

> suggested here - is something that ought not to be done without the most
> careful of reflection.
>
>  --karl--
>

---

John R. Levine johnl at iecc.com
Wed Apr 29 05:00:36 EDT 2009

* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

> As long as it takes. Otherwise we will have a system in which a mere
> accusation is sufficient.

Do you really think it is a good idea to require a court case and a trial
to take down a phish site pretending to be Paypal or the Bank of America?

You're quite right that among ICANN's less attractive qualities is its
tendency to invent half-assed processes dominated by lobbyists. On the
other hand, for every controversial high profile domain takedown, there
must be a thousand routine phish squashes.

If there's no formal process to do that, there will be informal processes,
and they're even more capricious than ICANN. Be careful what you wish
for.

R's,
John

---

Franck Martin franck.martin at gmail.com
Wed Apr 29 05:20:27 EDT 2009

* Previous message: [At-Large] ALAC Review Final Comments from the ALAC
* Next message: [At-Large] RAA, registrar "best practices, " bill of rights for users, etc.
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

Many social networks take down accounts based solely on report of violations of Terms Of Services.

I guess as long as a notice is served (your domain is terminated because violation of TOS, or better your domain will be terminated in 24 hours due to violation of TOS) and the domain owner has a right to answer the allegations or have its day in court, I'm cool with the process.

May be a bit like copyright take down notices, once notified, and after say 10 days, the registry becomes responsible for keeping the domain?

----- Original Message -----
From: "John R. Levine" <johnl at iecc.com>
To: "Karl Auerbach" <karl at cavebear.com>
Cc: "At-Large Worldwide" <at-large at atlarge-lists.icann.org>
Sent: Wednesday, 29 April, 2009 9:00:36 PM (GMT+1100) Auto-Detected
Subject: Re: [At-Large] Definition of registration abuse

> As long as it takes. Otherwise we will have a system in which a mere
> accusation is sufficient.

Do you really think it is a good idea to require a court case and a trial
to take down a phish site pretending to be Paypal or the Bank of America?

You're quite right that among ICANN's less attractive qualities is its
tendency to invent half-assed processes dominated by lobbyists. On the
other hand, for every controversial high profile domain takedown, there
must be a thousand routine phish squashes.

If there's no formal process to do that, there will be informal processes,
and they're even more capricious than ICANN. Be careful what you wish
for.

R's,
John

---

Karl Auerbach karl at cavebear.com
Wed Apr 29 05:49:29 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


John R. Levine wrote:
>> As long as it takes. Otherwise we will have a system in which a mere
>> accusation is sufficient.

>
> Do you really think it is a good idea to require a court case and a
> trial to take down a phish site pretending to be Paypal or the Bank of
> America?

How does one know that a particular web site is "a phish site pretending to be Paypal or the Bank of America"? Perhaps it is operating under a license? Perhaps it is a permissible parody.

We ought not to allow the takedown of things simply on accusation. There needs to be some process in which a impartial person takes a look at the facts and hears arguments. This need not be a heavyweight process.

Once the door is open for takedown by accusation then we've just handed every disgruntled person or over exuberant politico a means of causing trouble.

This is hardly a fantasy. We can look at the unjustified DMCA takedown claims and the heavyhanded Cease and Desist letters that have become routine tools by those who have highly inflated notions about the extent of their trademark and copyright rights.

Our history is full of periods in which simple accusation was translated into suppression - For instance in the early 1950's Senator Macarthy and his ilk ruined many innocent people by nothing more than unsubstantiated accusation.

The last election indicated that Youtube clips are going to be a big element of future campaigns. We can imagine that in the next election that opponents of a video will start to generate takedown notices on the most flimsily of grounds - perhaps on the basis of a trademarked name on a sign in the background or a bit of music that is drifted in during an interview. I suspect that it will get very nasty.

That's the kind of world we are going to end up with if we allow vigilante decisions to restrict the use of the internet.

--karl--

---

Derek Smythe derek at aa419.org
Wed Apr 29 06:36:30 EDT 2009

* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse

* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

Karl Auerbach wrote:
> John R. Levine wrote:
>>> As long as it takes. Otherwise we will have a system in which a mere
>>> accusation is sufficient.
>>
>> Do you really think it is a good idea to require a court case and a
>> trial to take down a phish site pretending to be Paypal or the Bank of
>> America?
>
> How does one know that a particular web site is "a phish site pretending
> to be Paypal or the Bank of America"? Perhaps it is operating under a
> license? Perhaps it is a permissible parody.

So by you argument this just might be the real Bank of International Settlements and Securities that is under construction:
http://www.biss-group.net

Or maybe not, just without secure protocols:
http://www.biss-group.net/biss/

Maybe they really are registered in Nigeria. Maybe the EFFC will really do something about this (despite thousand of similar sites they did nothing about).

And maybe real banks do use shared hosting along with 560 other websites and the regulators allow it.

Also, just maybe the are also a security company (http://www.biss-group.net/biss/home/sc.html) with other website predating it and registered before them have suddenly overnight decided it may be a great idea to plagiarize their content.

Maybe they have some weird SSL protocol they are using that nobody has ever heard about before:
http://www.biss-group.net/biss/home/onlinebanking/securesite001BISS/onlinebanking.php

Incidentally they just might be linked to Morgan Stanley whose image
http://www.biss-group.net/biss/home/images/morgan-stanley_loan_big.gif
is being used.

Maybe it may just be coincidence that this "banks" name is extremely close to the real Bank for International Settlements. However, since

the "banks" name is not identical, they are impersonating nobody. So all is good. Or is it?

I know otherwise, no surmises, no guesswork.

Obviously you would not use it, why subject more gullible innocent parties to it? There are parties here that see these on a daily basis. However if

It does not take a brain surgeon to recognize a scam, just some experience in the understanding of the scam.

May I challenge you and give you five domains to process by your methods? You decide if they are legitimate, how to process them etc?

Talk is cheap, but the victims to these are real.

Derek

---

Michele Neylon :: Blacknight michele at blacknight.ie
Wed Apr 29 08:35:57 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


On 29 Apr 2009, at 11:36, Derek Smythe wrote:
>
>
> And maybe real banks do use shared hosting along with 560 other
> websites and the regulators allow it.

Do financial regulators take into account hosting in their checks and balances? I somehow doubt it

We host a number of banks and financial institutions on shared hosting

for the simple reason that they are not transacting online
>
>
> It does not take a brain surgeon to recognize a scam, just some
> experience in the understanding of the scam.

Well maybe if the people reporting the scams were to send abuse
reports in English instead of techno-babble it might help

>
>
> May I challenge you and give you five domains to process by your
> methods? You decide if they are legitimate, how to process them etc?
>
> Talk is cheap, but the victims to these are real.

And I think you are conveniently missing the point entirely

If takedown notices etc., are not done properly innocent bystanders
can be impacted. If company X's CMS is on a machine with 500 websites
and
the cms is cracked / attacked / defaced which allows a phisher to put
up a paypal / Bank of whatever scam site, how would you like to see it
handled?

I suspect you'd want the site offline as quickly as possible...

Reality check - the hosting provider can't just pull the plug

>

Mr Michele Neylon
Blacknight Solutions
Hosting & Colocation, Brand Protection

---

Derek Smythe derek at aa419.org
Wed Apr 29 12:21:36 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


My reply inline.

Michele Neylon :: Blacknight wrote:
>
> On 29 Apr 2009, at 11:36, Derek Smythe wrote:
>>
>>
>> And maybe real banks do use shared hosting along with 560 other
>> websites and the regulators allow it.
>
> Do financial regulators take into account hosting in their checks and
> balances? I somehow doubt it
>
> We host a number of banks and financial institutions on shared hosting
> for the simple reason that they are not transacting online

Agreed. The example I chose deliberately showed the online transacting portion as well. These also do not reside on free shared accounts. I have been instrumental in many bank audits.

>>
>>
>> It does not take a brain surgeon to recognize a scam, just some
>> experience in the understanding of the scam.
>
> Well maybe if the people reporting the scams were to send abuse reports
> in English instead of techno-babble it might help
>
>>
>>
>> May I challenge you and give you five domains to process by your
>> methods? You decide if they are legitimate, how to process them etc?
>>
>> Talk is cheap, but the victims to these are real.
>
> And I think you are conveniently missing the point entirely
>
> If takedown notices etc., are not done properly innocent bystanders can
> be impacted. If company X's CMS is on a machine with 500 websites and
> the cms is cracked / attacked / defaced which allows a phisher to put up
> a paypal / Bank of whatever scam site, how would you like to see it
> handled?

That would depend on the potential harm. Sadly most people do not understand the difference between a 419 scam bank and a phishing site. Key is careful investigation.

If we talk phishing, most of these are hacks with a few exceptions. The immediate step is disabling access to the phish while preserving evidence. Most web servers allow that. That definitely does not mean the the whole website or server has to go. You may have to disable a feature or two to secure the server and prtect your other clients, also their potentially private data. I am sure you would agree.

>
> I suspect you'd want the site offline as quickly as possible...

The compromised site normally not, the phish yes - see above. Of course a follow up of how the breach occurred is important to avoid a repeat.

>
> Reality check - the hosting provider can't just pull the plug
>
No, however if the provider is happy he has sufficient evidence of the scam, he has his ToS/AUP to disable the scam site or contents. If he fails to enforce that, we can expect the one scam to become two, four eight ...

>>
>
> Mr Michele Neylon
> Blacknight Solutions
> Hosting & Colocation, Brand Protection

---

Karl Auerbach karl at cavebear.com
Wed Apr 29 12:51:01 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Derek Smythe wrote:

> It does not take a brain surgeon to recognize a scam, just some
> experience in the understanding of the scam.

Then it ought not to be hard to establish a procedure in which the facts and context of the accused scam is presented to an independent and disinterested third party, one who is familiar with the nature of these things, to review the situation.

> Talk is cheap, but the victims to these are real.

Accusations are even cheaper. And in many cases it is the one being accused who is the victim.

Who is the victim when a company uses takedown-upon-accusation to shut down a website that discloses the ill acts of that company? Who is the victim when the website of a labor union at a company is taken down upon accusation by the company that its trademark is being violated?

I had hoped that society had passed the shoot-now-and-ask-question-later stage.

There is a deeper aspect to this - which is that the internet has been lacking a protocol layer, one slightly above IP. It would be the mandatory identification and authentication layer. IPsec is there, but few use it even for protection much less for mutual identification and authentication.

--karl--

---

Derek Smythe derek at aa419.org
Wed Apr 29 16:04:42 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Karl Auerbach wrote:
> Derek Smythe wrote:
>
>> It does not take a brain surgeon to recognize a scam, just some
>> experience in the understanding of the scam.
>
> Then it ought not to be hard to establish a procedure in which the facts
> and context of the accused scam is presented to an independent and
> disinterested third party, one who is familiar with the nature of these
> things, to review the situation.
>

Exactly. You may be surprised at the depth of knowledge that could be found among the readers of these posts.

>
>> Talk is cheap, but the victims to these are real.
>
> Accusations are even cheaper. And in many cases it is the one being
> accused who is the victim.

What is the annual loss to cybercrime per year on the net?

The accused may not be a victim if proper research is done. In fact research that is given to a registrar on a plate in many instance proving a registrant has a fake addresses, is not who he says he is etc is ignored (RAA), yet is merril claims to be Abbey Bank of the UK/Natwest etc. The very same registrar will allow the registrant to register another domain with the proven non-exist address. That is the other side of the coin.

>
> Who is the victim when a company uses takedown-upon-accusation to shut
> down a website that discloses the ill acts of that company? Who is the
> victim when the website of a labor union at a company is taken down upon
> accusation by the company that its trademark is being violated?

I will definitely not argue with your logic here, since it is sound. Here we will have identified parties, not an internet highway mugger hiding behind internet anonymity. The situation is different.

However, there are well defined abuses, some of which I mentioned before. Also phishing which you mentioned before. However in you example you defied all logic and ignored what all the banks continuously warn their own client about.

>
> I had hoped that society had passed the shoot-now-and-ask-question-later
> stage.

Who is doing that? I would most definitely not approve of it either. I think you may be surprised with the degree of precision certain types of abuses can be defined, how they affect the general internet user which is supposed to be represented here. In fact most of these abuses are defined as criminal in many countries. If we wait until it is defined as criminal in all the countries around the world, it will never happen.

However since there are gray areas as you point out, does it mean we do not stop the actioning identified abuses since we dare not touch the gray areas. That is a bit like losing site of the forest for the trees.

That would not be representing the general internet user. That would in fact call into question other issues as well, opening up an even bigger can of worms. Everything we have today was started with a small step, using existing knowledge as a starting point.

>
> There is a deeper aspect to this - which is that the internet has been
> lacking a protocol layer, one slightly above IP. It would be the
> mandatory identification and authentication layer. IPsec is there, but
> few use it even for protection much less for mutual identification and
> authentication.
>
> --karl--
>
>
>
> _____

Derek

---

Evan Leibovitch evan at telly.org
Wed Apr 29 08:46:04 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Karl Auerbach wrote:
> John R. Levine wrote:
>>> As long as it takes. Otherwise we will have a system in which a
>>> mere accusation is sufficient.
>>
>> Do you really think it is a good idea to require a court case and a
>> trial to take down a phish site pretending to be Paypal or the Bank
>> of America?
>
> How does one know that a particular web site is "a phish site
> pretending to be Paypal or the Bank of America"? Perhaps it is

> operating under a license? Perhaps it is a permissible parody.

You're both right.

We can have guidelines set down -- that are adequately narrow -- to move in an expedited fashion. But even so, I agree that basic fundamentals of justice, such as the right to confront and challenge one's accuser, must be followed. Think of the process used to get a pre-trial injunction, which requires far more than a simple accusation but is not a full trial.

Legitimate players (parody, criticism sites, etc) should have a fairly easy and accessible process to challenge a preliminary shutdown order. Most bad players would take the site down and move on rather than challenge an accusation; they don't even want to be identified.

There can also be a regime in place that clearly indicates the disclaimer required by parody and criticism (ie, "this brand suck" sites) in order to provide an immediately recognized defence against preliminary takedown attempts.

The key, at least to me, is to continue to recall first principles of why trademarks were created -- to protect the consumer. If we continue to look at -- and press for -- the consumer centric POV of trademark protection, we'll be more clear and less defensive in our approach.

- Evan

---

Brendler, Beau Brenbe at consumer.org
Wed Apr 29 11:22:05 EDT 2009


* Previous message: [At-Large] Definition of registration abuse
* Next message: [At-Large] Definition of registration abuse
* Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]


Thanks for a spirited discussion on this. I am now trying to determine how best to aggregate these comments into the Registration Abuse Policy discussion. If anyone has particular privacy concerns, let me know.