

Forum:[Hack Forums](#)

Thread: [Extreme Internet Privacy](#)

AmericaOnline - March 5, 2018, 1:55 pm

Hi!

For the past two weeks, I have been attempting to completely erase all public presence of myself on the internet. These are the things that I have done so far:

1. Deletion of accounts that are shown in a Google Search - this has been very time consuming! I have probably deleted well over 40 accounts that I had created in the past (that Google had indexed). This involved a couple of phone calls, many, many emails, etc. For the accounts that I had forgotten the password to. Google has started re-crawling some of them, many of them no longer appear on Google.
2. Changing details - for those accounts that I could not delete or deactivate, I used Fake Name Generator [[w::ww::fakenamegenerator::com/](http://www.fakenamegenerator.com/)] to create a new identity to mask any evidence that I owned the account in the past.
3. I have opted-out of the 'open register' [[w::ww::gov::uk/electoral-register](http://www.gov.uk/electoral-register)] - this makes it harder for people searchers to find my address.
4. I have requested the removal of my information from 192 [[w::ww::192::com/people/](http://www.192.com/people/)].
5. I have requested that the information from the deleted accounts that is still indexed on Pipl [[pipl::com/](http://pipl.com/)] is removed - which it has.

As you can see, my efforts to 'reset' my internet presence has been quite extensive. If a person were to Google my name, they would only find the social media profiles of two people who have the same name as I do, along with two Google+ accounts from Google accounts that I have, unfortunately, forgotten the passwords to.

My question is: is there anything else that I can do to erase my public internet presence?

Thanks for the help!

Crystallize. - March 5, 2018, 2:55 pm

What's the point of this? You know you cannot be fully anonymous while surfing internet, you can be found with your IP.

SysAdmin - March 5, 2018, 3:02 pm

As long as you're using the internet, you're not going to be anonymous. You still have a subscription to the ISP that provides you with Internet Access, which holds your personal details anyway. Every website you visit will track you in some way.

AmericaOnline - March 5, 2018, 3:12 pm

(Mar 5, 2018 03:55 PM)Crystallize. Wrote: [\[CITE\]](#) What's the point of this? You know you cannot be fully anonymous while surfing internet, you can be found with your IP.

Thanks for the reply!

Do not be mistaken; my desire is not to remain fully anonymous online. I am not so naive as to believe that that is an easy feat for the ordinary citizen. However, what I do want to do is reduce the my online presence. What constitutes an online public presence?

1. Easy access to address.
2. Photographs of face.
3. Incriminating photographs.
4. Forum accounts linked to real name.

All of the above can be devastating to a person. All of them can contribute to a successful instance of identity theft. Access to one's address can enable others to locate you with ease - one may not want random people whom one met many years ago showing up on one's doorstep uninvited. Incriminating photographs can lead to reduced employment opportunities. Forum accounts that are linked to one's real name can help people to build an accurate picture regarding one's values, interests, etc.

For instance: a person is a member of a hacking forum and a mental health forum - it is easy to paint a picture of this person, and no matter how inaccurate it may be, it can lead to false, yet half-informed presumptions about that person. From these two forums, you might see this person as being unstable, possibly violent, anti-establishment, anarchist. When in fact, that person may enjoy innocent tinkering of computer systems, and have minor OCD.

You make the mistake in thinking that an IP address can be used as a concrete method of determining a person's identity - this is not true, at all. In fact, many services choose not to allow other users of that service to see the IP addresses of other users. Unless the IP address can be positively associated with an online account that details the person's name, age, address, ethnicity and gender, it cannot be used to paint a very substantial picture of that person.

If you have any more questions regarding my motivations, please do ask, otherwise, does anybody have any advice on how I can further pursue this?

Thanks :)

SysAdmin - refer to previous post. You cannot be "found" with your IP, unless that IP can be linked to accounts that have publicly available details regarding a person's identity. I took my IP and entered it into an IP -> coordinates site; the coordinates were about 5 miles away from my actual location.

With regards to ISP - I am 14 years old; the ISP is still in my parent's name. The ISP logs, unless compromised, are not available to the general public - they are often shared with government agencies and marketers. The former of which, by the way, is not my main concern - however, the way that the logs are likely processed is by coupling the logs to the ISP customers name - this is then placed into a government database. Compared to a person who uses an ISP that is paid for with a credit card in that person's name, I am reasonably safe.

\$ZEUS - March 5, 2018, 3:21 pm

You scared people will see your face? What about when you leave your house? How do you cover your identity then? I feel like wearing a mask would turn a lot of people off, especially in the world we live in today.

Incriminating photographs? Of what? Your pot use or affiliation to a sleeper cell?

BI1XY_H4CK3R5 - March 5, 2018, 3:23 pm

Hello Crystallize.

We are BI1XY_H4CK3R5, the points you have made in your post have become our main concerns & our main goals.

This is already happening by intel agencies and will continue to do so unless, the people as a whole try to make a difference.

What you are referring to is called Data Profiling and it is happening everywhere, even down to the adverts we are presented with.

Even in instances such as spoken interests then appearing as adverts on peoples facebook accounts. How? By users granting applications use of your phones features such as microphone, read messages, call logs etc under the belief that it is necessary. They listen to everything and soon enough they will know us better than we know ourselves. No information is safe online and once it is online there is no removing it, you may delete it for the eye to see but its hidden inside logs for future recollection by intelligence agencies.

AmericaOnline - March 5, 2018, 3:27 pm

(Mar 5, 2018 04:21 PM)\$ZEUS Wrote: [\[CITE\]](#) You scared people will see your face? What about when you leave your house? How do you cover your identity then? I feel like wearing a mask would turn a lot of people off, especially in the world we live in today.

Incriminating photographs? Of what? Your pot use or affiliation to a sleeper cell?

"What about when you leave your house" - people seeing your face in public is different to photographs of a person online. The permanency of the latter makes it dangerous - I hope I don't need to explain why.

If you are referring to CCTV - most CCTV cameras in operation do not make the images available to the public. They are rarely kept for as long as photographs on Facebook's servers are kept for.

Pot use is a very good example of an incriminating photograph. Especially in the UK, there is a lot of stigma surrounding the use of marijuana, especially by employers who see the users of marijuana as lazy, unproductive and criminal.

Thanks :)

(Mar 5, 2018 04:23 PM)BI1XY_H4CK3R5 Wrote: [\[CITE\]](#) Hello Crystallize.

We are BI1XY_H4CK3R5, the points you have made in your post have become our main concerns & our main goals.

This is already happening by intel agencies and will continue to do so unless, the people as a whole try to make a difference.

What you are referring to is called Data Profiling and it is happening everywhere, even down to the adverts we are presented with.

Even in instances such as spoken interests then appearing as adverts on peoples facebook accounts. How? By users granting applications use of your phones features such as microphone, read messages, call logs etc under the belief that it is necessary. They listen to everything and soon enough they will know us better than we know ourselves. No information is safe online and once it is online there is no removing it, you may delete it for the eye to see but its hidden inside logs for future recollection by intelligence agencies.

As I hinted in one of my previous posts, intelligence agencies are of little concern in this instance. It is possible to delete information from the eyes of the public - I have accomplished this (for the most part) in the past two weeks. I ensured that the accounts were not archived by the Wayback Machine too.

Another point is that, I do not feel comfortable having my data sold to third-party companies; not only do I feel 'used', but, if the data was leaked (as has happened in the past), people would have

great potential to blackmail people using the leaked information that may describe: porn habits, favorite dildo, political affiliations, etc.

Thanks! :)

BI1XY_H4CK3R5 - March 5, 2018, 3:37 pm

(Mar 5, 2018 04:27 PM)AmericaOnline Wrote: [\[CITE\]](#) "What about when you leave your house" - people seeing your face in public is different to photographs of a person online. The permanency of the latter makes it dangerous - I hope I don't need to explain why.

If you are referring to CCTV - most CCTV cameras in operation do not make the images available to the public. They are rarely kept for as long as photographs on Facebook's servers are kept for.

Pot use is a very good example of an incriminating photograph. Especially in the UK, there is a lot of stigma surrounding the use of marijuana, especially by employers who see the users of marijuana as lazy, unproductive and criminal.

Thanks :)

As I hinted in one of my previous posts, intelligence agencies are of little concern in this instance. It is possible to delete information from the eyes of the public - I have accomplished this (for the most part) in the past two weeks. I ensured that the accounts were not archived by the Wayback Machine too.

Another point is that, I do not feel comfortable having my data sold to third-party companies; not only do I feel 'used', but, if the data was leaked (as has happened in the past), people would have great potential to blackmail people using the leaked information that may describe: porn habits, favorite dildo, political affiliations, etc.

Thanks! :)

It is stored elsewhere, you can remove for the eye to see what you cant remove is the web logs on their side and if an agency was to request it you can be sure it will be handed over. I can relate to the third party point as we could be prosecuted doing the same thing although like already stated, this is already happening and although it may be of no concern right now, one question to throw into the air would be...

Would you rather some failed scam attempt from snippets of information or a successful prosecution of the state by which means evidence is irrelevant?

I know what id rather

AmericaOnline - March 5, 2018, 3:46 pm

(Mar 5, 2018 04:37 PM)BI1XY_H4CK3R5 Wrote: [\[CITE\]](#) It is stored elsewhere, you can remove for the eye to see what you cant remove is the web logs on their side and if an agency was to request it you can be sure it will be handed over. I can relate to the third party point as we could be prosecuted doing the same thing although like already stated, this is already happening and although it may be of no concern right now, one question to throw into the air would be...

Would you rather some failed scam attempt from snippets of information or a successful prosecution of the state by which means evidence is irrelevant?

I know what id rather

Absolutely, good point - people forget that, no matter how large the company is, mistakes (leaks)

happen - take, for example, AOL's leak [http://en.wikipedia.org/wiki/AOL_search_data_leak].

People also make the mistake of trusting governments to handle their data securely. They also make the mistakes of trusting governments to USE their data responsibly - possibly not today, but maybe tomorrow, a certain government may use whatever data they have to identify those whom they believe to be enemies of the state (I'm not talking about terrorists, I'm talking about gays under Hitler's rule type stuff).

Thanks.

Deany - March 5, 2018, 3:54 pm

if you're using an intel chip you're def being tracked

BI1XY_H4CK3R5 - March 5, 2018, 3:57 pm

(Mar 5, 2018 04:46 PM)AmericaOnline Wrote: [\[CITE\]](#) Absolutely, good point - people forget that, no matter how large the company is, mistakes (leaks) happen - take, for example, AOL's leak [http://en.wikipedia.org/wiki/AOL_search_data_leak].

People also make the mistake of trusting governments to handle their data securely. They also make the mistakes of trusting governments to USE their data responsibly - possibly not today, but maybe tomorrow, a certain government may use whatever data they have to identify those whom they believe to be enemies of the state (I'm not talking about terrorists, I'm talking about gays under Hitler's rule type stuff).

Thanks.

Exactly, they also make the big mistake in believing that all these mass produced devices from the likes of apple and google, are intended in an innocent matter. The only innocent things are the minds of the clueless users falling into that spider WEB

AmericaOnline - March 5, 2018, 3:58 pm

@Japanese -- Yeah, I know.

Once again, however, this thread is about online presence, not tracking, or the broader topic of privacy. Does anybody have any advice regarding further removal of personal data online. Does anybody have any other tools that I could be used to confirm whether or not I have any remaining profiles online. Are there any databases in the deep web that store data that might be linked to my identity. Any other ideas?

Thanks! :)

(Mar 5, 2018 04:57 PM)BI1XY_H4CK3R5 Wrote: [\[CITE\]](#) Exactly, they also make the big mistake in believing that all these mass produced devices from the likes of apple and google, are intended in an innocent matter. The only innocent things are the minds of the clueless users falling into that spider WEB

Too true. However, when people find what they believe to be refuge, they risk themselves even more. I'm not blaming DDG for anything, but few people do their research regarding services that supposedly offer "privacy". DuckDuckGo is hosted in the United States, and is therefore subject to the Patriot Act, it is hosted by Amazon (which is comparable to Google in terms of collection of personal data), and it is not a search engine, but a metasearch engine (it uses normal search engines such as Google) - not as safe as people think.

@BI1XY_H4CK3R5

It's a shame that the others aren't challenging our views - it could have made for a very interesting

(and enlightening) discussion.

BI1XY_H4CK3R5 - March 5, 2018, 4:06 pm

(Mar 5, 2018 04:58 PM)AmericaOnline Wrote: [\[CITE\]](#) @Japanese -- Yeah, I know.

Once again, however, this thread is about online presence, not tracking, or the broader topic of privacy. Does anybody have any advice regarding further removal of personal data online. Does anybody have any other tools that I could be used to confirm whether or not I have any remaining profiles online. Are there any databases in the deep web that store data that might be linked to my identity. Any other ideas?

Thanks! :)

Too true. However, when people find what they believe to be refuge, they risk themselves even more. I'm not blaming DDG for anything, but few people do their research regarding services that supposedly offer "privacy". DuckDuckGo is hosted in the United States, and is therefore subject to the Patriot Act, it is hosted by Amazon (which is comparable to Google in terms of collection of personal data), and it is not a search engine, but a metasearch engine (it uses normal search engines such as Google) - not as safe as people think.

There is a solution and thats to do what these criminals did to start with. You learn the very fundamentals of computers and code and you build your own services, reap what they offer and strive. Work together in unity and anything is possible, its just an illusion that it is not. And that illusion is that individually, we are "the little people" nothing more.

AmericaOnline - March 5, 2018, 4:21 pm

(Mar 5, 2018 05:06 PM)BI1XY_H4CK3R5 Wrote: [\[CITE\]](#) There is a solution and thats to do what these criminals did to start with. You learn the very fundamentals of computers and code and you build your own services, reap what they offer and strive. Work together in unity and anything is possible, its just an illusion that it is not. And that illusion is that individually, we are "the little people" nothing more.

I have often though about independent services for myself (namely personal email servers). However, there are certain disadvantages to this approach. One that might spring to everybody's mind is money - it is awfully expensive to purchase and maintain servers (as per the aforementioned example). The only way in which Google can afford its servers and employees to maintain them is through questionable acts such as data-broking and targeted-advertisement (among other things). Additionally, where would you store the server? One advantage of the Google data center is tight physical security - this would be difficult to replicate with a home-server and, as we all know, once the hacker has physical access to a system itself, your data is at massive risk of being compromised.

Really, building a private ISP is out of the question.

BI1XY_H4CK3R5 - March 5, 2018, 4:39 pm

(Mar 5, 2018 05:21 PM)AmericaOnline Wrote: [\[CITE\]](#) I have often though about independent services for myself (namely personal email servers). However, there are certain disadvantages to this approach. One that might spring to everybody's mind is money - it is awfully expensive to purchase and maintain servers (as per the aforementioned example). The only way in which Google can afford its servers and employees to maintain them is through questionable acts such as data-broking and targeted-advertisement (among other things).

Additionally, where would you store the server? One advantage of the Google data center is tight physical security - this would be difficult to replicate with a home-server and, as we all know, once the hacker has physical access to a system itself, your data is at massive risk of being compromised.

Really, building a private ISP is out of the question.

It is not something we are definite on as of yet but we take pride in hoping that someday we may be able to put together an adept group of people that manage to figure this thing out. After all, people can be remarkable, tech is continually advancing and being a hacker is all about the possibilities not the linear design. It would be pretty cool to have you jump on board to invest your contribution and the best thing about working as a group is that the possibilities you may miss, will be picked up upon by somebody else in most cases. There are many protocols to still be explored and there are no doubt multiple vulnerabilities in them too, but once those vulnerabilities are exploited who knows where they may lead us.

AmericaOnline - March 5, 2018, 4:49 pm

(Mar 5, 2018 05:39 PM)BI1XY_H4CK3R5 Wrote: [\[CITE\]](#) It is not something we are definite on as of yet but we take pride in hoping that someday we may be able to put together an adept group of people that manage to figure this thing out. After all, people can be remarkable, tech is continually advancing and being a hacker is all about the possibilities not the linear design. It would be pretty cool to have you jump on board to invest your contribution and the best thing about working as a group is that the possibilities you may miss, will be picked up upon by somebody else in most cases. There are many protocols to still be explored and there are no doubt multiple vulnerabilities in them too, but once those vulnerabilities are exploited who knows where they may lead us.

Humans are, by their very nature, greedy. No matter how passionate I may be about internet privacy and freedom, there will always be a price on one's moral values. We do not know what incentivizes some technology companies to release user information to intelligence organizations, however we cannot be so naive as to believe that you would not give-in to the same kind of enticement. Additionally, people are so used to the internet being gratis; if a person wishes to use a service that does not sell user information, they should expect to pay a premium - there aren't many people who are willing to pay \$10 a year for their security and privacy - there are other logistical problems that spring to mind too.

La Vida Loca - March 5, 2018, 4:49 pm

Lol writing a thread like this is certainly not a good move when attempting to hide your online presence

AmericaOnline - March 5, 2018, 4:52 pm

(Mar 5, 2018 05:49 PM)La Vida Loca Wrote: [\[CITE\]](#) Lol writing a thread like this is certainly not a good move when attempting to hide your online presence

I was thinking the same thing however, surprisingly, "AmericaOnline" is not my real name.

Int Ptr - March 5, 2018, 10:58 pm

People seem to be completely missing the point of this thread.

XwhoXamXiX - March 26, 2018, 3:01 pm

I think there was a good tutorial on detracting yourself by Marxist .. hope it helps