Anonymity Online: Is It Possible to Not Leave a Trace?

Description

Given that close monitoring online (online surveillance) now begins at an early age, digital hygiene should be well taken care of ever since one's childhood.

There seems to be an illusion with the inexperienced internet users that only some individuals are being closely monitored and secretly 'surveilled' online. An ordinary user tends to think that to secretly monitor and listen to an unsuspecting online user is too costly and complicated and that one particular individual, he or she i.e. a simple user, is not particularly interesting to anybody to be listened to or closely monitored at all.

But the facts have no mercy; data storage and information saving are nowadays rather affordable and so called 'big data' about each user has been being saved continually for about eight to ten years now, because those who closely monitor us, cannot possibly know what and who a student of today will be in ten or fifteen years (for instance a member of Parliament, a high-ranking civil servant, a successful businessman or perhaps what position the current middle level employee will hold in three to four years and who he or she will work with in the future.

To closely monitor hundreds of millions of users in the form of online surveillance is technically possible nowadays and it is not prohibitively expensive so that it is being done by many individuals in the USA and globally.

There are so called 'markers' – sensitive points, points of interest – which are determined by way of automatic procedures of mass data processing. Data analysis is at present rather inexpensive. Those individuals who perform the close monitoring of others are not even particularly interested in any particular individual precisely, but by means of the information conversion into its impact – on whom out of a huge number of users in the form of online surveillance in the course of years and years of close monitoring compromising data can be collated on this person's relations, weaknesses, tendencies etc.

Thus, each individual should be wary of his or her own digital hygiene, especially a civil servant, a politician, a manager, a business person, a high-visibility person, or a celebrity and a person of high repute in any area of interest, that is, all those who already can be viewed as the risk group and who

are already subject to close monitoring (surveillance) and influence. Given that close monitoring online (online surveillance) now begins at an early age, digital hygiene should be well taken care of ever since one's childhood, because the collated compromising material about any child being simply prone to some mischief typical of a child, will be 'precious' at his or her adult ripe age, when the child of today becomes an adult, mature person who may well change their own views of the world in due time.

It is obvious that close monitoring (surveillance) online of people of significance is being carried out meticulously and in great detail, and complete with planting trojan horse programmes into one's computer by blending all the channels of communication together by monitoring his or her immediate digital vicinity.

This new digital reality of literally total visibility and high risk calls for new rules of digital hygiene.

Anonymity: Is It Possible to Not Leave a Trace?

Person 1*. Hello, is this the anonymous phone number of the FSB?*

Person 2. *Yes, Mikhail Petrovich, yes it is. We are here for you. What would you like to tell us?*

Internet users seem to think that they can keep their privacy and remain anonymous and invisible if they so wish, entering the online network via anonymous accounts under the disguise of their avatars and nicknames, using various ***anonymizers*** which hide their own IP address, virtual private VPN networks which hide one's IP address, private virtual addresses, entering the web via TOR network, without any police or special services cannot recognize this 'cunning' user and/or closely monitor.

There is some partial truth in it though. It is possible for a person to exist without being noticed and act in digital space if one possesses the knowledge and expertise of a professional hacker or a digital spy. Fortunately or not, this body of knowledge and habits are unavailable to most of the users.

An ordinary user continually leaves his or her own digital trace, which can use for his or her certain identification if there is interest to do so and with the appropriate tools,

Signature: Digital Fingerprints

Using digital devices with internet access, we continually, with each moment in time, create unique 'digital fingerprints' and traces of our actions and of our digital environment. These are called 'signatures' (from its Latin linguistic root to sign).

For instance, in geoanalytics, there is the rule of four points based on which ones you tend to visit most often one can analyse your personality. One point, for example, the underground station near your home is visited by tens of thousands of people with smartphones in their pockets and at the same time, two points: one in close proximity to your house and another point in immediate vicinity to your work are visited by just a few thousand people. Three points – two underground stations and your favourite restaurant – now the number narrows down to only a few dozens of people with smartphones in their pockets. And if they add your mum's address, to which you go once or twice a week or the address of your gym – you will be the only person with that combination of geographical points you go to.

That is your individual geographical digital signature, your own 'digital fingerprint'. Such digital signatures are aplenty and these get to be decoded by a huge number of those who closely monitor

you (online and digital surveillance of a person).

Your browsing history i.e. the list of websites you visit on a daily basis forms your unique digital ‘impression’ of your browsers (search engines) both in the logs (journals) of your browsers, as well as the cloud of its producer and also in countless marketing and advertising systems and ‘the counters’ on the internet.

It might be possible that for your own unique accurate identification there need not be four websites being visited but for instance fourteen but that is not that relevant.

As a general rule, if the vector, which is a set of digits, made up of the traces you leave behind you (the geographical points, the website you visit, downloaded apps) is long enough, it defenitely identifies you perfectly well without any doubt. For example, if you post statuses on social media with an anonymous nickname, in that case you form a minimum vector of dates in time and the exact times these were posted and the comments and even regardless of their contents).

From the point of view of the internet provider you form one particular time vector = the dates and the times of going online.

The first vector is known by the users of social media – the platforms and the surveillance programmes for close monitoring of social media. The second time vector is known by your home internet provider or your mobile operator, which does not see your social media posts, but as a general rule, is familiar with your personal identity.

By way of blending and crossing these vectors for instance upon the formal request of legal investigation authorities (such as law enforcement, the courts of justice etc), one’s allegedly anonymous identity can be decoded relatively easily.

Yes, all the vectors of all the internet users will have to be viewed more closely and compared with the vector of your social media posts. This task is rather technical and can be resolved pretty easily with the internet servers of today and their technical capabilities.

All in all, one should bear in mind that your unique digital signature consists of:

1 factory identifier IMEI of your smart phone

2. the list of apps and files on your device such as your laptop or your mobile phone which is available to many devices and apps, your antivirus, your computer viruses and your Trojans, your browser, your operating system, your office apps and all the office apps of your colleagues etc
3. your Bluetooth environment – all the devices your Bluetooth gets in touch with to share data or which it has ever got in touch with and joined digitally, your music devices at home or in your car, your ear phones, your voice tools etc.
4. your Wi-fi environment – a list of all the Wi-fi devices around your place of work or your home.
5. your browser history – a list of the websites and internet services you regularly visit
6. your list of friends on social media – your social impression is unique even if you decide to use a pseudonym to go online. That list exists with the social media platform as such, and with all the ‘monitoring’ programmes and in your browser as well.
7. your lexical signature – a group of your favourite words, phrases and sayings, and even a unique combination of your common typos

8. your face and faces of others on your photos and videos on social media – a combination of all the faces including yours among others, is also a unique identifier.
9. your geographical signature – a list of your routes and geographical points you go to, either in your own city or outside. It exists in your navigator or your navigation apps
10. your voice signature – your voice digital footprint or 'impression' you leave either while using your mobile phone or the microphone on your laptop.
11. your search list key words – apart from the situational keywords to search depending on the situation, there are regular search keywords you often look up and type in, and their combination is certainly unique i.e. your own, and it exists on your favourite search engine and browser.
12. your list of favourite topics – for examples in the news portal
13. a list of the devices in your neighbourhood – for example, your internet provider 'can see' which other mobile devices are normally in the immediate vicinity such as your family members or close colleagues.

And the list goes on. All these signatures are saved in your smartphone and in a huge number of those independent viewers unrelated to you (advertising systems, mobile operators, internet providers, browsers, search engines, social media, online platforms, apps etc).

If by any chance some signature is missing, during the process of identification, other signatures can be added among those listed above, and then that combination will definitely be unique: your own combination.

What we have just pointed out above means that even an anonymous user on the web leaves his or her unique digital traces and 'footprints'. If you have two accounts, one for regular communication under your real name and another one which is anonymous, rest assured that these can be automatically connected by analysing their signatures.

to be continued

– an excerpt above from a book ***Digital Hygiene*** *(???????? ???????) translated into English by* ***Tatiana Obrenovic***

– the original book Digital Hygiene (???????? ???????) was written in Russian by Igor Ashmanov and Natalya Kasperskaya, Moscow State University (??????????? ?????????????? ???????????)

by Tatiana Obrenovic
Category

1. Freedom-Free speech-Resitance & H-rights
2. Main
3. Science-Tech-AI-Medical & Gen. Research

Date Created
04/20/2023