International Journal of Innovative Research in Electronics and Communications (IJIREC)
Volume 5, Issue 4, 2018, PP 1-4
ISSN 2349-4050 (Online) & ISSN 2349-4042 (Print)
DOI: http://dx.doi.org/10.20431/2349-4050.0504004
www.arcjournals.org

Governments Failure on Global Digital Geopolitical Strategy

Christos Beretas, Msc

Corresponding Author:** ***Christos Beretas, Msc, *PhD Candidate in Cyber Security at Innovative Knowledge Institute, Paris, France*

Abstract: *Governments think they have the capacity and ability to control the origin of information and its validity, but no one can guarantee the integrity of the information and how it came about. Many people believe that people who have authority also have control and power, this is not the case, control, power and authority is given to the one who has the knowledge and information to carry out his/her purpose with the right choices.*

Among us there are companies, public and private for different purposes, companies can be set up by non-friendly countries of high interest to gather information. The goal remains the same, the creation of a digital profile with the habits and needs of people who are in the research and interest field. Of course this is not only possible in the physical world but also in the digital world.

In the digital world it is very easy to create a digital human profile when you are even on the government side it is easier because then there is Internet Service Provider (ISP) support so the candidate's digital footprint can be easily searched. But even when you're not on the government side, companies with the right technology can trap the prospective victim to build their profile online.

So governments around the world aren't the only ones who want to know the habits of citizens, but what happens when governments themselves fall victim to it?

Keywords: *IoT, Goovernment, Security, VPN, Proxy, Surveillance, Networks, Technology*..

1. INTRODUCTION

How many times when someone browse internet does an ad message appear for something he/she had been searching for a long time ago? How many times browsing the web without downloading a file suddenly redirects to another website, it is often the phenomenon is increasing over time.

How many times have users reported being prompted in various ways to visit fake websites or clone websites? How many times has it happened for computer users to report that after a safe internet browsing, a virus has been downloaded to their computer without being able to even understand how it went downloaded? How many times have we noticed the point-tracking service either on PC applications or on mobile phones? How many times have users reported receiving emails that are either targeted at them by mentioning the recipient's last name or trying to entice users to open the message after the subject of the message is addressed and is on in both of the above cases the purpose is for the recipient to open the email and execute the attachment, and here's how complicated the thing is, the cases are **3,** the first case is nothing happens, the drop of services that either owe to a remote server is in a different implementation of the recipient's operating system, the second case is to infect the recipient computer with some kind of virus that will cause file loss, the third case is by executing the file of an email nothing visible to the user while in the background if it steals everything from the user's computer, it can run for years without ever realizing it. Who could be behind all the above challenges? the governments? companies operating on behalf of government agencies or governments? Private companies that want to manipulate governments? the answer is, they could be partial yes but also all together.

The digital age has invaded our lives, information systems infrastructures are incomplete because technological developments are galloping with slower networking and security infrastructures, many countries around the world do not even have a strategy to deal with cyberattack, governments, companies, and ordinary users find themselves at the forefront of events, unable to cope with threats that are often impossible to trace.

The world is changing, will security change?

2. WHY GOVERNMENTS FAIL ON GLOBAL DIGITAL GEOPOLITICAL STRATEGY

Governments around the world want to control digital information in every way, this is usually done on the grounds of crime prevention, this is not necessarily wrong. But what governments around the world cannot control is technological development, digital technology, software development, and finally human ingenuity. No government can foresee human ingenuity, what for governments around the world that may be considered impossible for somebody else.

In order for governments to gather as much information as possible about every person they care about, they are employing every possible means at their disposal, naming what is feasible for them that they think will be able to gather the knowledge they need to create as close as possible. digital profile of the person who is interested. The collection of information can be from anywhere, as points out, from metadata, from mobile networks using user information and then mobile data, data networks and social media data. Smart devices known as **IoT** can be easily targeted since their metadata tracking is easy so then daily logging functions can be ported to these smart devices, this is something that could work for years without the slightest suspicion from the ordinary user that something is wrong Also, gathering information in this way can be focused not on the collection but on the storage of information, tthat is, in cloud systems where information is centralized and easier to analyze. Companies also have access to such systems, which can actually work for this purpose, namely on behalf of foreign governments or business interests. The centralized information is something that both sides love very much.

Internet service providers are a good starting point for the immediate collection of information of the target users, there is a state-level advantage over a private company, and this is because a government can easily pass a law so it can restrict, monitor, interfaces, and installs networking software and hardware into the equipment of Internet service providers, so gathering information is very easy, as every user connect to the internet leaves traces behind for the websites they browse and online activity. Someone might think, yes we know all this and we are using anonymous Proxy Servers and VPN, the answer is that they are not secure because nobody know the real side of the company that offers these services if it holds personal data and then passes it on to government, also all of these anonymous service providers nobody really know in which states have their Servers and also don't know the legal framework that applies to anonymity in every state. Companies involved in analyzing information could if they wanted to use this personal data if permitted by the legal framework of a country, in addition, they could also access ISPs data not directly but indirectly, simply by help employees who have access to personal data and just want an extra income by satisfying the information needs of some companies that deal with it on behalf of third parties.

Governments have the potential to become flexible through legislative frameworks, they can present online applications to third parties, but by using them they could collect so much data that by their very nature they could create a virtual profile, and vice versa. But a company on behalf of a third company could create or lure by making online clone services while luring even government agencies and even citizens. In digital technology there are no borders and knowledge is shared across the world, without the legal power governments would constantly be a step backwards. Social media networks as mentioned above is a good source of information mining, we could say is a free and open source of information. There, information management and extraction tools can be easily developed through the API. Users of social media networks for instant communication and easy-to-use management environments to complete their profile enter as complete as possible their personal information, for example, upload photos, share travel locations, walking hours, the time they have fun, their location, personal moments, phones, and other personal information. Collecting information from open sources is a job that is very much loved by those who are involved in collecting information from open sources. It is very easy to create a digital profile of a person with open source data only.

Automated tools are an important tool on both sides, by means of automated tools we mean those tools that collect information from users while they are browsing the internet, either in the form of automated programs ie **Bots** that will try or collect information. either they will try to infiltrate remote systems in order to gain access to those systems and then spy on information. Detecting intruders managed by the Bot is an extremely difficult and complicated process, while finding those websites that collect information without the knowledge of their users is considered a difficult process because these tools can be hidden from users and furthermore users do not know from which website exactly their personal data was leaked, if they ever realized it.

It is worth noting that both in the case of governments and in the case of private companies Honeypot websites operate that advertise for something else in essence all they do is collect personal information and then distribute it to the stakeholders. Never trust service providers that offer anonymity services. I would be very skeptical if a government agency implemented an anonymity system at the moment that government agencies are interested in collecting classified information. Who could assure that between the nodes of the network running secret and encrypted communication, there is no contradict a state intelligence service, or one company who is involving in information analysis? An even worse scenario is that the whole anonymity service is designed and implemented to collect and analyze information.

I would like to point out that both parties are interested in information that is closer to their physical form, namely non-encrypted information that will produce results quickly and easily. Such information can be extracted from open data sources as mentioned above, from ISPs, from information systems, metadata, and finally from the Cloud. The Cloud is a very good source of data input, since governments can order the transfer of files that are still there, and they can also order the decryption of files there in accordance with existing legislation. In addition, many applications running on the Cloud do not encrypt their information, so it is easy to extract this information either legally or by violating the system, or by deliberately leaving a back door on the Cloud platform.

Someone might think, "VPN is a worthwhile and only anonymity option", nowadays it is very difficult to find a reliable and secure VPN service provider. Rapid technological innovation has led many governments around the world to seek out information and habits for Internet users to be able to know the characteristics of each user by even creating digital profiles with user habits. The challenges are many, the governments in the name of security go beyond any legal obstacles and go on to breach privacy because they want to learn the directions of a society, politically believes, and generally have in their possession data to manipulate situations. On the other hand, users who is looking for internet freedom they choose VPN services from various random providers, most of all ignoring the quality and security of the provided services, this is due to the search for private communication and internet freedom, but that is something that needs a lot of work and it certainly will not be the governments that will contribute to it.

There were once **5** eyes, then **9** and now **14**, of course not referring to a humans eyes, I refer to digital eyes, is the number of countries around the world who have joined and agreed on the exchange of information. Most of them are made up of European countries, while several Asian countries have been involved. More and more users and people actively engaged in the security of computing, networks, privacy and VPNs security have begun to raise their concerns more and more. It is also natural that fears arise from this system of online mass surveillance, which restricts the freedom of citizens. Concerns are constantly increasing in the potential violation of privacy that may arise through our internet activity using a VPN service. The first thing is about to think that we need to use VPN services that do not use any infrastructure that is located in the 14 countries with an active information exchange agreement, several VPN services advertise that, this as an asset but again the final user does not know whether there is an network node between the user and the VPN service that passes the information through one or more network infrastructure nodes from the 14 surveillance countries. We should not forget that if the VPN provider is based in a country of 14 eyes, may be be asked to deliver the customer data. By law, is compelled to comply. However, a VPN service provider can defend itself by not logging the online activities of the users, this is rarely happen because of the legal problem that will arise if a users uses the VPN for illegal activities, if this happens, it will put the company in a very difficult position. VPN service providers should choose to operate in countries that fully apply the privacy of information and do not succumb to pressure; such a country is Switzerland where data protection and privacy are not negotiated. However, using a VPN service is not anonymous as web browsers leave behind online footprints that are unique and can help identify a user. So a user can be found among millions of users, and an online activity can be monitored without the use of cookies.

Undoubtedly, a VPN service provides more security and privacy than not using any VPN. Information spying methods are evolving, which means that VPN service providers should also develop their services using additional security measures without the help of government agencies while also examining their legal dependencies and obligations against the country where they are providing services and operate. The VPN service provider who does not cooperate in any case with government agencies and is based in countries that do not participate in the information exchange program of 14 eyes, the country where it is

based supports the freedom of communication and supports privacy and finally monitors the activity of the users but does not transfer this data to the government, these personal data will be presented ones and only as a presumption in a legal dispute that preceded a malicious act where they will be presented alone the relevant case-related data and nothing else, if the above is observed, the market itself will show the most reliable provider that offers security and privacy to its clients.

3. CONCLUSION

According to the present research, it is abundantly demonstrated that the simple user cannot protect his/her privacy, is confronted on both sides by governments and companies that collect and process personal information. Governments that are in turn confronted with information gathering and analysis companies and vice versa are also helpless. Governments have therefore lost the momentum of data collection exclusivity and are at risk of spying on foreign governments either by domestic companies operating either autonomously or on behalf of third parties. Users should always forget about anonymity on the internet, there is no anonymity on the internet, there is false anonymity as well there is wrong configuration or a deliberately wrong configuration so that anonymity services can somehow be managed in order to enjoy the anonymity of the internet. No government agency in the world would want a completely anonymous online service for the simple reason that it could not interfere with the collection of classified information, so important projects would fall into disrepair. The next time someone offered anonymous online services or if you believe the internet is used anonymously, think again.

REFERENCES

[1] Matthew Bailey. 2015. Complete Guide to Internet Privacy, Anonymity & Security.

[2] Kathy Furgang. 2017. Internet Surveillance and How to Protect Your Privacy (Digital & Information Literacy).

[3] Glenn Greenwald. 2014. No Place to Hide.