Volume 6, Issue 1, 2022 ISSN: 2617-4537
DOI: https://doi.org/10.31058/j.data.2022.61007

The Impact of Social Media in Privacy and Their Role in Decision Making

Christos Beretas[1*]

[1] Cyber Security at Innovative Knowledge Institute (Paris Graduate School), Paris, France

Email Address

cberetas@ikinstitute.org (Christos Beretas)
*Correspondence: cberetas@ikinstitute.org

Received: 25 November 2021**; Accepted:** 25 March 2022**; Published:** 29 July 2022

Abstract:

Social media has been rumored in recent years, with social media not only referring to the popular but also the less popular, as well as targeted social media, including the collection. and analysis of information which information is then used for other purposes. Social media offers users plenty of features and smart features using artificial intelligence while making the most of the internet. Through the use of social media, it is possible to manage and view information from smart devices, also known as IoT. This implies on the one hand freedom of interfaces and freedom of operations and on the other hand implies an increased risk of privacy violations combined with the possibility of illegal access and control of smart devices. Various countries around the world have created cyber armies that use a variety of techniques - including social media - to monitor, suspend, and internally influence the functioning of states and directly influence decision-making, and generally intervene in the operation in another country, a typical example is the deepfake of politicians using social media to influence public opinion. As a result of the large amount of personal data that users themselves enter in various ways on social media is the source of information that can be exploited and used for other purposes including marketing. There is no clear indication of who is actually the owner of this information, in many cases there is a difference from the terms of use of the services and the national legislation of the country in which a social media company is based or have the facilities there. which are entered into social media databases are never deleted, the deletion of personal information by the user should not be considered, for example the deletion of photos given, should be considered an invisible and not deleted permanently. This contributes to the exchange of information with government agencies and the creation of electronic profiles of people and their habits. Social media does not have the same impact on the public, the reasons are many, such as for example there are people who know what happens to personal data, so they are skeptical about the content they choose to share on social media, others users avoid the use of social media, other users due to social beliefs avoid the use of social media. On the other hand, social media offers tempting applications and functionality to the users in order to bend as much as they can the most skeptical users using applications and services of artificial intelligence in order to bend any problems that arise. Users seem to be indifferent to what is really going on from the use of their personal data. In the boom of communication and the intelligent possibilities offered by information technology, the sectors, privacy, security, and digital freedom of people are sacrificed as social media does not offer access to their users regarding the collected personal data, nor is it given to them users to set the collection of personal data they want. Due to socialization and globalization, social media has become necessary for the socialization of people, so it can be considered that there is a human consensus for the violation of his privacy which is socially legitimate. In the future there is expected to be a new condition for the defined privacy as the facts of the time change and the definition in new orders of things must be adjusted.

Keywords:
Social Media, Privacy, Surveillance, Violation, Decision Making, e-Profile

1. Introduction

The use of the social media platforms becomes more intense over time with a plethora of new functions and applications. Many of the social media are used as a professional tool by various companies and organizations either for the promotion of products and services or for the extraction of data and the collection of open information. In the majority of social media, required by users to create a profile, enter and confirm either their personal email address or their mobile phone number, a practice that generates questions, with the most important question being whether it is possible behind a profile to identify the human factor and to record his/her associations, for example, way of life, habits, etc. Also, using social media, the user and profilemaker is not the only one who enters personal data in his / her profile, but also automatically enters meta-data related to various habits and information that is derived from the information entered by the social media user. On social media it is practically impossible to know the person on the other side, maybe there is someone with mental problems or another government official who purposefully wants to collect as much information as possible from the suspected victim. The reckless use of social media can become idiosyncratic for the following reasons, the addiction, in this case a person avoid the dangers that exist and is permanently located on a computer screen and uses the same tools. On the other hand, behind a social media profile can be hidden someone with psychological problems or a government employee after first creating a fake account trying to collect personal information which will later be used for various targeted purposes, such as creating riots in a country by presenting on social media high-ranking government officials to spread false news which will lead to a popular uprising. It is very important to understand that social media are systems that can be attacked at any time, this could be a further breach of personal data and leakage to third parties. One has to take seriously the possibilities of locating users, a feature that is available through social media, one might think that locating users limited to a city name is not dangerous, but no one knows internally in information systems and databases that reach the level of user tracking which may not be visible to users but to record with absolute accuracy the exact location of the user. The previous report on the dangers of locating is very important as it can greatly help information analysts locate important information about the user, information such as, frequency of visits to comparable locations, travel and return times, people who comment / mention /follow /connect / support, the hours of absence from home or work, habits, etc. The above are some important entities, which assist in the collection and analysis of information from open sources in order to more easily achieve the creation of e-profiles of users. Social media can be addictive, as can social outbursts of hatred and resentment if used as a means of hybrid warfare to exploit third countries' internal weaknesses in order to impose their own interests and beliefs. It's the easiest way to publish a fake video, a deepfake product that other users will unknowingly republish and quickly get a lot of publicity and switch from one social media to another by adding the appropriate hashtag #hashtag.

2. Analysis

Many people worry that social media is stealing or intending to steal their freedom. These people who think the above are not irrational and do not make completely wrong thoughts. Social media can be seen as responsible for policy and choice making, that is, it can influence decision-making and influence people greatly by making wrong decisions, taking into account perceptions that did not exist or have a different meaning from those presented in the social media networks. Deepfake's technique flourished growth to the proliferation of social media, enabling people to manipulate other people, governments to influence other governments to manipulate them. Public opinion is reluctant to believe, on the one hand there is common sense, and on the other a video that presents some facts that affect public opinion, because the image is more faithful than logic and thought, the people are manipulated and persuaded about what they see, simply by presuming that they saw with their own eyes and believed what they saw. For this reason, deepfake has made great progress and is widely used today to influence any entity whether it is an ordinary citizen or an adversary government, or the target country. Detecting deepfake is not an easy process, technology has made it relatively easy to perfect a fake video that looks like a real one, capable of affecting a large portion of the people. This technique is also used by the hybrid war, which without the use of real weapons, with the appropriate communication strategy, the necessary tools, and social media are capable of influencing and inciting even rebellious whole peoples against in their governments, is capable of inciting certain categories of citizens causing internal sabotage within target countries, infuriating and inciting citizens against their governments,without demanding any military intervention as would be the case in a real rather than a hybrid war.

The personal data that exists on social media that has been retrieved on them in any way, such as input by the users themselves, meta-data, personal data that has been retrieved on social media networking platforms by applications, are all information that is available from open sources. Depending on the origin and the goals, anyone can use this available information from open source for various reasons such as, targeted advertising, digital profile creation, blackmail, targeted interventions, etc. Note, that there is no clear legal framework that specifies the minimum exposure of users' personal data on social media, but even if it did exist, there are several methods of collecting personal data from social media that actually control personal data collected seems impossible.

Anonymity that can be applied to the internet in various ways, of course, does not mean anonymously creating a fake profile on the internet, anonymity is the inability to locate the real person behind a digital profile as it is impossible to locate because of the great restriction in its digital footprints. This feature allows skilled users to create fake profiles by completely hiding their information using deceptive IP addresses to browse the internet and social media anonymously, tracking, blackmailing, or collecting personal information from targeted third-party accounts. The reaction of social media at this point is limited, the reason is that even if the connections from anonymous proxy servers or the TOR network are restricted or banned, there are thousands of infected computers and information systems that can be used as anonymous proxy servers so that savvy users can cover their traces. The above is a technique used to gather information from open sources but also in hybrid warfare. In hybrid warfare, the above process is carried out in a more methodical and group way, hybrid warfare does not have the desired effect when it is not carried out by individuals, it has the desired results when it is carried out by groups.

Another crucial question about social media is privacy and ownership of information. The content that users upload to social media even when it is explicitly mentioned and the personal data in the terms of use, is not able to prove that this information - data where is actually stored, who else can access in them, if after deletion by their user they still remain in data warehouses invisible to the user, to whom these data belong, and by what legal framework and country they are governed. The further processing of personal data and the storage of users' personal data in countries that are not known to users makes users skeptical about the use of social media. A social media platform that could be used for advertising or monetary purposes could sell this information to third parties, but in order not to be overlooked by users, it would sell limited information so that sensitive information could not be perceived by the users themselves. This also implies a violation of human rights, as part of their personal life and personal information are available for different purposes for which they were given. Therefore, the users themselves can receive these ads with different content so that it is not possible to detect the sale of their personal information. Another violation of privacy is the possibility of reading personal messages from third parties or even from Bot, many times in the boom of security the privacy is sacrificed, so in the name of security are established terms and conditions so that the violation of privacy is legal.

The privacy of social media should in no case be given either to personal data which was registered by the users themselves as mentioned above, or they were registered automated by various other methods such as automated applications which as mentioned above, also in various other ways such as Tracking cookies, and social media networks that operate as honeypot projects.

Let's analyze the first part which concerns tracking cookies. Tracking cookies are used by social media networks to identify the users which are browsing on social media networks where they can track them. These tracking targets as much as possible the display of targeted ads by recording the posts made by users on their profiles, the locations they are on, the searches they perform on social media, and finally tracking cookies may be used while remaining active for third party websites. from the operation of these websites the monitoring of the users can be expanded. On the other hand, there are Honeypot projects, these are fake social media networks (platforms) which have appeared and disappeared and have taken their place, new, created either by government agencies targeting citizens of certain countries to control the activities of users and to contribute In tracking specific users, such social media networks were also introduced by hackers as well as government agencies who wanted to create competitive social media networking platforms that enabled users to even receive a paid new sign-up bonus, cheaper payments in users 'ads in order for users to enter their credit or debit card number and then proceed to deduct amounts of money greater than the expansive cost, read users' personal messages ignoring the ownership and privacy of communications and in some cases the user could find a personal message posted on the internet without of course mentioning the origin of the message or the name of the user.

All of the above acknowledge how social media users need to be extremely careful not to be indifferent to their privacy and personal information. Do not subscribe to unknown and dubious social media networks (platforms), especially those social media networks where information, user registration is selective or even posts are filtered and there is no real freedom of speech.

3. Conclusions

According to what was mentioned in this article, conclude that social media on the one hand contributes to the further socialization of people, contributes to business development, user interaction, artificial intelligence is applied, there is increased potential for targeted advertising, businesses have the ability to be promoted globally by creating social media profiles most of the time for free, while there is the ability for businesses to interact with their customers by interacting with applications offered by social media platforms. On the other hand, social media accumulates and processes a significant amount of personal information, users' personal data is stored forever, users do not have access to their personal data, users do not know in which countries their personal data is stored, who owns this personal data if it has been stored to social media databases, they do not know if this personal data is used for publicity purposes or is shared with government agencies for analysis. In conclusion, users should create profiles on social media networks only in those that they deem absolutely necessary, with as little information as possible from users, upload and share as little content as they can, and do not use applications offered by social media which for their use presuppose the consent of users to access other private information.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this article.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

References

[1] Christos, B. How Really Secure is TOR and the Privacy it Offers. Nanotechnology and Advanced Material Science, 2020.

[2] Christos, B. Cyber Hybrid Warfare: Asymmetric threat. Journal of Nanotechnology and Advanced Material Science, 2020.

[3] Christos, B. Governments Failure on Global Digital Geopolitical Strategy. International Journal of Innovative Research in Electronics and Communications, 2019.

[4] Christos, B. Security and Privacy in Data Networks. Research in Medical & Engineering Sciences, 2018.

[5] Christos, B. Internet of Things and Privacy. Journal of Industrial Engineering and Safety, 2018.

[6] Christos, B. Cloud Computing and Privacy. Journal of Electrical & Electronic Systems, 2017.