

## Article

# Social Media Data Misuse

Tariq Soussan<sup>1</sup>, Marcello Trovati<sup>1</sup>

<sup>1</sup> Computer Science Department, Edge Hill University, UK. Emails: [tariqsoussan@gmail.com](mailto:tariqsoussan@gmail.com); [marcello.trovati@edgehill.ac.uk](mailto:marcello.trovati@edgehill.ac.uk)

**Abstract:** The present high-tech landscape has allowed institutes to undergo digital transformation in addition to the storing of exceptional bulks of information from several resources, such as mobile phones, debit cards, GPS, transactions, online logs, and e-records. With the growth of technology, big data has grown to be a huge resource for several corporations that helped in encouraging enhanced strategies and innovative enterprise prospects. This advancement has also offered the expansion of linkable data resources. One of the famous data sources is social media platforms. Ideas and different types of content are being posted by thousands of people via social networking sites. These sites have provided a modern method for operating companies efficiently. However, some studies showed that social media platforms can be a source for misinformation at which some users tend to misuse social media data. In this work, the ethical concerns and conduct in online communities has been reviewed in order to see how social media data from different platforms has been misused, and to highlight some of the ways to avoid the misuse of social media data.

**Keywords:** Social media ethics, Social media, data misuse, data integrity

## 1. Introduction

The growth of technology has transformed the lifestyle that people lead. However, it has also created major issues of over population, societal difficulties, and ecological obstacles. Ethical aspects are coming to be extremely valuable despite of progressively serious demographic, societal and ecological concerns [7]. There are many incidents that happened in the world recently that require users to highlight and rediscover the ethical aspect in technology [8]. Ethics have advanced as an essential aspect of technology with its expansion. Technology requiring morals is a fundamental necessity for itself and it is primarily divided into 3 parts. The first part explains that the technology excellence is eventually assessed by nature and it adds that nature and technology should be compatible. The second part describes that the openness of technology verifies the technology must be controlled. Lastly, technology morals deliberateness is continuation contrast to the use of technology. Thus, an essential aspect of technology is its ethical aspect and for technology to grow, there is an inexorable need for ethics [7]. Because of several developments in technology, as well as the growth of smart gadgets, the cloud computing rising, and the internet of things, big amounts of data are produced every day at an outstanding pace from various sources such as wellbeing, regime, social networks, advertising, and business [5]. The objective of creating technology is frequently to get it to fulfill a specific purpose [1]. Technology and its purpose have a clear and uncontroversial correlation. Technology maintains ethical consequences irrespective if the technology has been produced with this considered or not [1]. To be capable of managing the function and

ethics during the design procedure is an aim and far-reaching desire [1]. An example of an ethical problem related to technology is in China during which the technologies that are being used in big social engineering schemes with social media and face recognition have been used to generate a worldwide 'social-credit' scheme [29]. This scheme improves the social status and benefits of people based on a mark which the authority system appoints as a measurement of their social integrity. This is defined as their capability to encourage a scheme of "social coherence" [29].

Overall, the designers need to predict as much usage situations as can be while planning technology so that they can foresee any potential ethical obstacles [1].

Big sets of data were collected from digital detectors that detect signals or stimuli, networks, computation, and memory receiving information devices which are of significance to industry, science, administrations, and organization. New companies were established on obtaining free to access information on the internet and delivering it to individuals in beneficial ways. Microsoft, Google, and Yahoo are examples of such businesses [25]. New facilities like satellite pictures, steering instructions, and picture recovery are added by such corporations that gather loads of bytes of information each day. While search portals have changed how data can be retrieved, the actions of corporations, scientific scholars, medical physicians, and security and intelligence functions have been altered by additional types of big data computing [25]. In the coming sections, section 2 will discuss the social media data misuse. Section 3 will discuss the data misuse in Facebook platform. Section 4 and 5 will discuss the data misuse in Twitter and Instagram platforms, respectively. Section 6 will discuss the data misuse in LinkedIn platform. Section 7 will discuss some of the ways to restrict social media data misuse.

## 2. Social Media Data Misuse

Social Media data is now shared by millions of users who spread information and provide online point of views. Users of social media platforms can disregard or unfollow points of views that do not fit their own contrasting local network [21]. Corporations use social media platforms to distribute data about the goods and services proposed by them [14]. In current years, a rising issue appeared related to how social media networks are being utilized for propaganda and false campaigns [10].

These platforms host customer discussions, prospects, and points of views. Using current online platforms through robot accounts and remote users may introduce misinformation into social media, generate a fad, and promptly propagate the message in a quicker and less expensive way than any other channel in the past [21]. Beneficial choices can be achieved and collaborations between customers and shareholders can be reached when corporations use those platforms [17]. Discussions on cooperation social media profiles effect the choices the cooperation can make. With ethical conduct and company social obligation, organizations can longstanding receive substantial longstanding profits, yet occasionally the corporations may become engaged with the unconventional methods leading to quicker, short-term benefits [15].

By fabricating data on social media, organizations can fraudulently invite clients to their goods, improve sales and revenues, invite additional workers, and decrease enrollment expenses. On their clients' engagement in social media, organizations can generate various analytics to be used in profit making business approaches [15]. The technology ethical side lead to a modern research area called Technoethics. Technoethics means technological morals. In the technological intelligence framework, AI and robotics areas are confronting vital ethical judgment which has made technoethics grow to be more valuable [7]. Posted data on social media can lack authenticity and profile pages may contain accessible personal information [15]. In addition, there are other risks that may arise from social media. Intruders, trolls, and psychopaths contact victims through social media [12]. Child safety concerns are raised because some users may harass kids and young individuals online [18]. Due to failed political revolutions, some regimes have intensified management of social media platforms [23]. Moreover, these platforms, can encourage terrorist actions and distribute rumors in tragedy circumstances [2]. Those examples of data misuse have resulted to intensified supervision of civilians and online networks. Other problems exist when users try to embrace dangerous information other users have posted or when they adopt harmful conduct other users have done or when they adopt abuse of personal data with illegal intention [16]. An example about this is online forums where users post about their experience. There is a possible risk if wrong, useless, or even dangerous information is posted on those discussion forums [16]

There are several moral concerns in social media that ought to be considered in spite of its practical and valuable ability in the social and progressive evolution in human interaction [15]. One concern is data anonymous. Organizations receive fake customer product feedbacks which are false and could harm the reputation of organizations. Some social media networks allow users to remain unknown during which their identity is switched to a number or an icon, so users will not realize who they are speaking to [28].

### **3. Facebook Data Misuse**

Facebook is a social media platform that allows users to socialize, interact, and post pictures and videos. It has shown some issues which cannot be disregarded. With regards to privacy of personal information, devices that have its application installed and permissions approved, allow the application to assemble data and log on to services, as per the data policy, such as time zone, Wi-Fi Signals, mobile operator, ISP, GPS, language, Bluetooth [27]. In such a case, the data being collected by Facebook cannot be controlled by users. In addition, some immoral Facebook posts that might include sentiments containing racism, or religious hate have led to Facebook to fulfill governments' requirements to prevent or limit massive amount of user contents in some countries [11].

In terms of information leakage, details about eighty-six million people who use Facebook were distributed by a researcher to a political organization specialized in consulting called "Cambridge Analytica" which dealt with the campaign of Trump [6]. Another issue that Facebook faced was identity theft. Identity theft occurred when a user builds a fake account to copy the someone's identity or when a user hacks someone's password and impersonates the owner of the account [15]. Furthermore, an additional issue regarding Facebook data is fake news as Facebook has more shared fake news reports than famous mainstream news reports [24].

### **4. Twitter Data Misuse**

Twitter social media platform has also foreseen some unethical behaviors during which its data has been misused. Fake accounts on Twitter can produce junk email, false web rating, and false information. Fake accounts may also be used to disclose prohibited download links and stalking other users through those accounts [15]. Some corporations used Twitter to exhibit their undesirable goods into people's timelines through paid tweets. Other issues related to Twitter data was the tweets' absence of context which occurred when Twitter users misread the messages because of the absence of all the vital information related to a concept which may be confusing [19]. Moreover, another ethical dilemma with Twitter is ghost tweets of which people hire ghostwriters to use their Twitter accounts and tweet as if it were them. The problem here is that the tweets content truth or falsification cannot be known by users [15]. In addition, there was another was selling Twitter data for commercial benefits.

### **5. Instagram Data Misuse**

Another social media platform that had some social media misuse was Instagram. Like Facebook, Instagram also allows posting and sharing pictures and videos. In the terms and conditions, it is compulsory for users before joining the network to accept that their private pictures on the platform can be acquired by main advertising organizations or third-party purchasers without their approval [15]. There is an official and legitimate approval needed from Instagram users for Instagram to reach private data, nonetheless,

users sometimes tend to agree on the permission forms before reviewing them [3]. Thus, this might jeopardize the users' private data being sold. Moreover, another issue regarding Instagram data misuse is influencer digital advertising. Businesses expect that customers will be more persuaded to seek the goods or services that the corporation proposes when these businesses display influencers on Instagram to the marketplace they are aiming for, [9].

## 6. LinkedIn Data Misuse

LinkedIn is a professional social media platform where users create profiles having their employment and private data which is shared with other users. LinkedIn also had some unethical problems. The platform has a job board that company owners can post job offers related to their company. However, some companies have advertised vacancies that do not exist because they want to collect information such as archive of CVs and create traffic on their LinkedIn webpage [15]. In addition, businesses must pay money to LinkedIn for vacancies posted and for accessing the CVs [15]. The accuracy and the reliability of LinkedIn data cannot be verified. Previous work has showed that 50% of CVs used to evaluate job candidates by HR specialists can include factual faults [20].

When studying the conditions for doing employment through LinkedIn platform, absence of legal guidance was observed which is another issue related to the platform. Incorrect procurement may occur if HR specialists are not trained on how to retrieve online data since they might be hiring new employees based on false acquired information [15]. Another issue with LinkedIn platform is the absence of privacy. Companies are collecting data about potential candidates before a job is offered. Their employers use this data through LinkedIn to perform screening checks prior to recruitment [22].

## 7. Approaches to restrict Social Media Data Misuse

A survey from previous work showed that the social media job screening performed by corporations in the United States for job candidates has risen to 70% in 2018 after it was around 11% in 2006 [10]. The companies tend to authenticate applicants' skills, evaluate if they introduce themselves in a professional way, and guarantee that these applicants do not have any posts that can be categorized as bullying or insulting content [10]. Thus, when employers or hiring managers have the chance to reach such "reliable data", it can be referred to as cybervetting [4]. This kind of data can help determine crucial metrics, such as academic capability and job efficiency [13].

Since not all users are acquainted with the methods relating to their social media data being misused or breached, they found this to be a barrier for them when they want to use social media. Some previous work proposes that beginner users are aided by a facilitator or well internet knowledgeable tutors so that those users can get familiarized with data confidentiality safety concerns and other important data [16]. Although some social media websites guide their new users throughout registration, the conversations and content being shared may not be strongly checked by a moderator. Users with little knowledge prefer to have a moderator who can they return to if they have some queries [16].

Moreover, Policymakers need to read, envision, and cross-examine how the analytics from social networks can be integrated ethically, thus worries of individuals and businesses are looked after [15]. The objective and the extended consequences of the analytics of social media is vital to be recognized by the policymakers. Businesses need to build, distribute, and regularly employ specific rules concerning its utilization of analytics of social media [15].

In businesses, there are certain approaches for trying to reduce exploitation of social media data by workers. Social media misuse can take place beyond the physical sites of the businesses, in nonworking hours of the employees, and can be done by any device

regardless of, if it belongs to the company or not [26]. Thus, it is vital for companies to deliver proper employee training related to the rules, and data security and equality law in specific to try to reduce the harm that can be produced by social media platforms data misuse [26]. Another approach that businesses can apply is usage policies for social media. It includes the guidelines of conduct required from workers which are related to their usage of social media in a clear way regardless of if they are at the workplace or not [26]. Another approach is related to the use of companies' official social media accounts. There should be rules on creating such accounts in addition to updating and supervising them. Access to those accounts should be limited to authorized employees only [26]. Any references used on these accounts should be cited as per copyright law. Moreover, another strategy for avoiding social media data misuse is following some guidance. An example is for employees to update their accounts from public accounts to private accounts, thus only users on their friend list can see their posts' content taking into consideration that the friend list is reviewed often [26]. Employers should offer guidance to try to guarantee that workers are considerate about their company, their colleagues, and others that might be correlated with the company.

..

## 8. Conclusion

In this work, the possible misuse of social networking platforms has been reviewed. Many examples were given from previous work about how social media have been misused with focus on data misuse coming from social media platforms such as Facebook, Twitter, Instagram, and LinkedIn. Many suggested approaches have been mentioned to deal with such data misuse. To restrict or minimize misuse, certain usage rules need to be applied. Providing beginner users with some tutoring can help them get to know more about data confidentiality safety concerns and other information that might help them. Future work can suggest more ways on making stakeholders aware about the misuse of their social media data so that they can take the necessary precautions to keep their data safe from being misused.

## References

1. Albrechtslund, A. (2007). Ethics and technology design. *Ethics and information technology*, 9(1), 63-72.
2. Alexander, D. E. (2014). Social media in disaster risk reduction and crisis management. *Science and engineering ethics*, 20(3), 717-733.
3. Bechmann, A., & Vahlstrup, P. B. (2015). Studying Facebook and Instagram data: The digital footprints software. *First Monday*.
4. Berkelaar, B. L. (2014). Cybervetting, online information, and personnel selection: New transparency expectations and the emergence of a digital social contract. *Management Communication Quarterly*, 28(4), 479-506.
5. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, 56, 684-700.



6. Cadwalladr, C., Confessore, N., & Rosenberg, M. (2018). How Trump consultants exploited the Facebook Data of Millions. *The new York Times*.
7. Fan, Z., & Ge, Y. (2018). The Influence of Technoethics on Industrial Design. In *MATEC Web of Conferences* (Vol. 167, p. 01008). EDP Sciences.
8. Galvan, J. M. (2003). On technoethics. *IEEE-RAS Magazine*, 10(4), 58-63.
9. Glucksman, M. (2017). The rise of social media influencer marketing on lifestyle branding: A case study of Lucie Fink. *Elon Journal of Undergraduate Research in Communications*, 8(2), 77-87.
10. Gruz, A., Jacobson, J., & Dubois, E. (2020). Cybervetting and the Public Life of Social Media Data. *Social Media+ Society*, 6(2), 2056305120915618.
11. Isaac, M. (2016). Facebook said to create censorship tool to get back into China. *The New York Times*. Retrived from <http://www.nytimes.com>.
12. Kim, W., Jeong, O. R., & Lee, S. W. (2010). On social Web sites. *Information systems*, 35(2), 215-236.
13. Kluemper, D. H., Rosen, P. A., & Mossholder, K. W. (2012). Social networking websites, personality ratings, and the organizational context: More than meets the eye? 1. *Journal of Applied Social Psychology*, 42(5), 1143-1172.
14. Kumar, P., & Mittal, S. (2012). The perpetration and prevention of cyber crime: an analysis of cyber terrorism in India. *International Journal of Technoethics (IJT)*, 3(1), 43-52.
15. Kumar, V., & Nanda, P. (2019). Social media to social media analytics: Ethical challenges. *International Journal of Technoethics (IJT)*, 10(2), 57-70.
16. Leist, A. K. (2013). Social media use of older adults: a mini-review. *Gerontology*, 59(4), 378-384.
17. Naik, D. A. (2015). Organizational use of social media: The shift in communication, collaboration and decision-making.
18. O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, 127(4), 800-804.
19. Onook, O., Manish, A., & Raghav, R. H. (2013). Community intelligence and social media services: A rumor theoretic analysis of tweets during social crisis. *Management Information Systems Quarterly*, 37(2), 407-A7.
20. Pare, M. E. (2013). Linked into a job?: The ethical considerations of recruiting through LinkedIn.
21. Prier, J. (2017). *The Command of the Trend: Social Media as a Weapon in the Information Age*. SCHOOL OF ADVANCED AIR AND SPACE STUDIES, AIR UNIVERSITY MAXWELL AFB United States.
22. Saylin, G., & Horrocks, T. (2013). The risks of pre-employment social media screening. *SHRM*. [online] Available at: <<https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/preemployment-social-media-screening.aspx>> [Accessed 27 February, 2019].
23. Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign affairs*, 28-41.
24. Silverman, C., & Singer-Vine, J. (2016). Most Americans who see fake news believe it, new survey says. *BuzzFeed news*, 6, 2016.
25. Syed, A., Gillela, K., & Venugopal, C. (2013). The future revolution on big data. *Future*, 2(6), 2446-2451.
26. Taylor, M., Haggerty, J., Gresty, D., Wren, C., & Berry, T. (2016). Avoiding the misuse of social media by employees. *Network Security*, 2016(5), 8-11.
27. Thompson, C. (2015). What you really sign up for when you use social media. *CNBC*.
28. Turculeț, M. (2014). Ethical issues concerning online social networks. *Procedia-Social and Behavioral Sciences*, 149, 967-972.
29. Vallor, S., Green, B., & Raicu, I. (2018). Ethics in Technology Practice. *The Markkula Center for Applied Ethics at Santa Clara University*. <https://>