ISSN No:-2456-2165

Privacy Concerns and Ethical Prospects in Modern Software Architectures

Alexandru Marius Obretin, Andreea Alina Cornea*
Department of Economic Informatics
Bucharest University of Economic Studies
Bucharest, Romania

Abstract:- Information technology has known a steady and continuous growth in the last decades, being the driving source of innovation, modeling the present and shaping the future. However, besides its indisputable benefits, novelty in the realm of information technology brings security concerns and dangers for which a large segment of the population is yet unprepared. This paper aims to analyze the risks regarding data privacy, integrity, and security in various economic contexts and to provide guidelines for ethical prospects in the software solutions of the future.

Keywords:- *data privacy; data integrity; ethics;*

I. INTRODUCTION

Since the beginning of what would be later known as the dot-com bubble more and more entrepreneurs and technology enthusiasts have challenged the way things used to be done, created new platforms, services and means that pursued one goal - to make life easier. From online shopping to booking platforms, internet banking, streaming services, social media platforms, cloud services, entire infrastructures accessible on demand, solutions that provide geolocation, ride sharing applications, online conference platforms, all intended to change the old world for the better.

These innovations brought the third industrial revolution and determined job extinction for two sets of activities. On the one hand, repetitive tasks got automated by robots, entire computerized warehouses being built all over the world, where machines can extract, pack, and deliver merchandise without human interaction. On the other hand, a particular category of businesses encountered a more convenient substitute. Stores that used to sell music albums are now extinct, since people started listening to music on online services like YouTube, Apple Music, Deezer or Spotify. Albums acquisition happens currently directly from the Internet. Similarly, movie rental stores have been replaced by so popular nowadays streaming platforms like Netflix, HBO Go, Disney Plus, and Amazon Prime. Once large and profitable businesses inherently went bankrupt.

These days the most powerful companies in the world are technology companies. Some of them sell products, like Apple or Tesla, some of them created very cost-effective business modes like Amazon, while others are just bringing innovation through software - for Google, Facebook or Microsoft most of their profits come from applications and services they invented.

The world is currently more connected than before, people can interact with each other basically anytime they want, and some sort of technology dependence has been settled down, as the trend is irreversible.

II. DATA DRIVEN THREATS

To state it from the beginning, this article is not going to present things in black or white. Often, they are colored in shades of gray and the long-term goal should be to determine the causes, to understand the consequences and ultimately to act consciously. It depends on each individual which of the following resonates the most: Increased use of technology exposed people to more diversity and knowledge, bridging society. Increased use of technology left room for hate speech, racism and damaged the relationships inside communities. Technology made people feel connected. Technology made people feel lonely. Yet, what it is sure is that disruptive technologies repercussions for society are and always were hard to predict.

Still, a reference study, taken by awarded human development psychologist Patricia Greenfield on the effects on intelligence and learning ability the exposure to various types of media has, suggested that increased use of technology “widespread and sophisticated development of visual-spatial skills”, but simultaneously reduced the capacity for “mindful knowledge acquisition, inductive analysis, critical thinking, imagination, and reflection” [1]. A tendency to remember where information might be accessible when needed, instead of memorizing important ideas has been identified. An experiment conducted by neuroscientist Ian Robertson noticed that elder people are more capable of recalling personal information than the youngsters. The participants were asked to tell a relative’s birth date and while 87% of the subjects over 50 could answer, only 40% of those under 30 were able. In addition, only a third of the latter category knew their own phone number [2]. Although these findings are provoking, the more interesting story this study tells is in the long run these behavioral changes might possibly alter our predisposition to analyze information from different sources and derive compound conclusions. The critical thinking might end up being undermined by shallow engagement because of reduced attention spans. As the author Nicholas Carr explained in his book “The shallows”, the process of enriching thinking follows a certain sequence. When people discover new ideas, they firstly get stored in a limited, temporary, and volatile working memory. Further, the information is transferred to the long-term memory, a more persistent and roomy area inside the brain, where it is digested, correlated with already available knowledge, and integrated into complex thoughts. But the working memory is sensitive, and its content vanishes as soon as the attention gets distracted, similar to the random-access memory inside a

ISSN No:-2456-2165

computer that loses all the information during a power outage. Moreover, when the cognitive load the working memory operates with exceeds its limited storage capacity, the transfer to the long-term memory is restrained, with consequences for learning [3]. This overload might be a result of long-time exposure to technology, to social media in particular, because the attention gets bombarded with an endless flow of digital stimuli in shapes of pictures and videos that continuously provides something new, something different which interferes with sustained concentration.

Dopamine-driven feedback loops integrated in most social media platforms have been inspired by the same psychological principles that create engagement in slot machines. This gratification system that constantly gives the users carefully tailored content to arouse emotions keeps them captive in infinite scrolling for more and more distraction, social validation, and outrage. Cognitive neuroscientists revealed that rewarding social stimuli can trigger the dopaminergic reward pathways inside the brain in a similar manner to drugs [4]. The downside of this constant pursue for more happiness is the exposure the social media users get to an often filtered, deceiving portrayal of daily experiences. Some of them start feeling social anxiety, inadequacy in respect with their peers, they doubt themselves, become irritated and undervalue their personality. The fear of missing out is making people believe they are left out and do not belong somewhere.

Beside this psychological impact, improper use of technology might lead to an even more concerning aftermath. As Alison Wood Brooks, an assistant professor at Harvard Business School, highlighted in an interview about the implications of digital communication on the sense of belonging for Harvard Medicine magazine "people are plugged in all the time, which means we can track behavior and cognition precisely and carefully over time" [5].

And while most of the people neither are aware about this fact, nor have given explicit consent, they use apparently free services in exchange for their data. Because when a service is free of charge, it is not the end user the real customer, but the marketers, the advertisers, those willing to pay for the opportunity to persuade the users to act or believe in accordance with their interests. Statistics show that only between 3-9% of the respondents read the terms and conditions when using an application [6]. For example, as of December 2021, The Independent online newspaper has a list of 143 different companies they might share user data with and some of those entities are able to exploit the data for purposes like the ones in Figure 1.

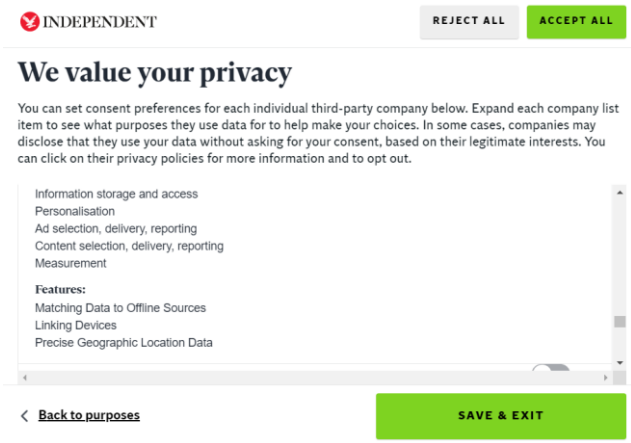

Fig. 1: The Independent's vendor list

It is written in plain text these companies can use the information without asking for consent to create user profiles, to understand what users read, where they live, what kind of devices they use. Therefore, the two billion users registered to Facebook are the sold merchandise, rather than a meaningful community. And the customers' interests are not always noble. Recent years showed how social media became a playground for computational propaganda and what raises concern is the nature of the phenomenon. Most valued companies on Earth spent tremendous resources in the last decades crafting addictive platforms able to provide adaptive, personalized content. Contextually, this can also be read as propaganda, unfortunately. Gillian Bolsover and Philip Howard noticed three ways in which social media and the Internet has influenced propaganda. Everyone connected to the Internet has currently international-scale propaganda access one click away, whereas geographical limitations have been removed. In addition, automation grants efficiency in spreading misinformation and anonymity assures the source is protected and facts are hard to verify [7]. Scandals like Cambridge Analytica brought into attention practices like social media micro-targeting and what is striking is that people involved in such practices talk free and easy in interviews and streamed conferences about playing with people's fears and emotions in an attempt to manipulate, to influence their attitude. Alexander Nix, the CEO of Cambridge Analytica, detailed in a 2015 interview for Bloomberg: "Your behavior is driven by your personality and actually the more you can understand about people's personality as psychological drivers, the more you can actually start to really tap in to why and how they make their decisions. We call this behavioral microtargeting" [8]. And while Cambridge Analytica is the most notorious name in the realm of big data backed psychographics, they are certainly not the only one. A research article published in the Proceedings of the National Academy of Sciences used Facebook likes as input data in a model capable of assessing human character. The results speak for themselves. With just 10 likes the algorithm developed by Michal Kosinski, a PhD candidate at Cambridge at the time, can guess someone's behavior better than an average colleague. 70 likes are enough to provide better accuracy than a friend. With 150 input entries, the algorithm outperforms a family member. 300 likes provide a better behavior prediction than the subject's partner [9]. When the results were published, SCL

ISSN No:-2456-2165

Group, a company specialized in psychological operations for the military, tried to purchase the algorithm from Kosinski, but he refused, and the company found someone else for the job. The alternative – a personality test that required an authentication with Facebook - built by Aleksandr Kogan, a fellow Cambridge professor, exploited an opportunity in Facebook's public API and harvested information not just from the subject that took the test, but from his entire friends list. And the collateral targets of the test had no idea about the process. The data collected by Aleksandr Kogan's survey led to Cambridge Analytica establishment.

Christopher Wylie, a former research director and the whistleblower that denounced the practices used by Cambridge Analytica in front of the court, described in his book how they combined micro-targeting, which already existed in politics, with new constructs from psychology to target individuals as personalities, rather than voters. The result will underline what messages a subject is susceptible to in terms of topics, content, tone, framing, when the subject is likely to consume a message and the frequency such messages need to have in order to progressively change subject's opinion. He claims, besides the research and development departments, Cambridge Analytica also had entire teams of content creators that outlined proper messages for certain types of subjects and targeting teams that delivered them through the Internet using purposely designed blogs and websites [10]. What data has been collected about everyone is yet hard to say, as the company refused to disclose the information garnered about David Caroll, an American citizen who sued Cambridge Analytica to reclaim his data and currently an online privacy speaker and promoter.

Further studies revealed the phenomenon is extending far beyond the exploits of social media platforms public APIs. Jonathan Albright, the research director for Columbia University's center for Digital Journalism, analyzed 117 websites known for spreading fake news in the context of United States presidential elections in 2016. The graphical representation of their interconnection describes the magnitude and the manner of spread misinformation. The researcher noted "these sites created an ecosystem of real-time propaganda: they include viral hoax engines that can instantly shape public opinion through mass reaction to serious political topics and news events. This network is triggered on-demand to spread false, hyper-biased, and politically-loaded information" [11]. But beside the existence of this apparatus and the immediate consequences, what is more concerning is how it used to collect data about the persons who access such websites. From 114 out of the initial 117 entities Jonathan Albright saved about 200 megabytes of resources that are downloaded on the client side, resources that get stored on personal computers, smartphones, and tablets of those who visit the websites. According to his blog post, he indirectly connected to 474 third parties representing "behavioral tracking companies, sketchy advertising networks, social network APIs, AddThis sharing buttons, data mining outfits, and content delivery providers" [12]. Some of these third parties turn out accessing personal details about the users - they find out where people live, where they work, which places they visit, what things they buy, what things they like, who are their friends, their families, their colleagues, whether they are religious or followers of certain ideologies, details about their health condition, expressed opinions on social media, financial profiles and so on. The treacherous side of this practice is it goes beyond the scope of that website. Users visit a link and data about their lives starts getting collected. And the data is not limited to that domain only. The more expressive they are in arguments, in comment sections, the more precise personal profiles they end up having, while those interested in the profiles sit back, under the radar and send messages that trigger emotional reactions, as modern technology facilitates content creation on a large scale. A different experiment from the same Jonathan Albright explored the realm of deep fake and the impact it has on a streaming platform like YouTube. The findings are thrilling as 19 different channels uploaded 78349 videos starting with the phrase "A tease" – a marker for videos created using artificial intelligence, some of these channels posting new videos every 3 minutes [13]. Nevertheless, deep fake has become a serious concern recently as the latest technological progress allowed creation of fake media that is indistinguishable from reality where apparently legit individuals say or act in ways that never happened.

Despite this factual exhibition, one interesting feature that is worth emphasizing about technology is the difference in velocity when comparing the amplitude of the evolution and the time span needed for it. Basically, in one generation society transitioned from the dawn of the information age and the first personal computers to the extent where electronics are incorporated in household appliances, robots explore the universe and artificial intelligence applications defeat world's best players in Go. Though, one important aspect is that technological evolution has affected multiple generations simultaneously. And while youngsters are more prone to digitalization, since some of them take contact with this connected world from an early age and learn about the possibilities the information technology offers, there are generations that experienced digitalization quite late in their lifetime. Therefore, the latter category sometimes struggles to keep up with the changes, considers hard to continuously adapt and occasionally feels alone when people around tend to get absorbed by some game or funny video on social media [14].

Equally relevant, there are different levels of understanding information technology. On the one hand, some people are passionate by the phenomenon, they follow bloggers, attend lectures and study thoroughly, but on the other hand, more just do not understand the underlying principles. Withal, the degree of digitalization is not uniformly spread across the world, since developed countries, usually the promoters of novel and ingenious innovations, are more digitalized compared with developing countries, where hotspots of digitalization are met preponderant in large urban areas, while rural communities usually lack.

These facts support the general idea that profound changes require extensive transition periods. People feeling overwhelmed by technology are neither familiar with the circumstances, nor properly exposed to them. Consequently,

the same category hardly understands the risks it exposes to when using the Internet. One step further on the causal relationship, technological illiteracy encourages large number of cybercrimes. Their frequency and impact have raised drastically in the past years and according to the Ninth Annual Cost of Cybercrime Study improper cybersecurity protection measures would let 5.2 trillion USD at risk over the next five years, globally [15]. Following, a closer look over the article where The Economist argued data have become the most valuable resource on Earth, surpassing oil, would be appropriate [16].

III. INDOOR POSITIONING CONTEXT

Lately, most of the challenges outdoor location raises have been addressed and currently popular software applications allow precise geolocation, profitable business being created on such flexibility. For example, Google Maps can identify someone outdoors with several-meter precision, social media platforms like Snapchat let users know where their peers are and Waze is able to determine in real time traffic jams, developing a crowd-sourcing business model. Yet, indoor location is still uncharted, and companies invest large amounts of money to secure competitive advantage and gain more market share over their competitors. The indoor positioning market is expected to grow in the following decade with a compound year over year rate of 30% [17].

Current approaches used in indoor location might be split into two categories. One is relying on external hardware infrastructure and uses Bluetooth Low Energy, Near Field Communication, Wi-Fi signal, magnetic field detection or dead reckoning. They usually imply higher initial costs and are affected by exterior noise generated by highly dense areas. The other is software based and quite often relies on smartphone capabilities like sensors or camera. Some implemented solutions capture video streams using the camera and compare them with already known reference models relying on image recognition techniques, others involve artificial intelligence for indoor displacement determination using inertial measurement units' data from the built-in accelerometer and gyroscope [18], [19].

Indoor positioning systems are expected to optimize processes in facility management, warehouses, large shopping centers or public institutions. Routing algorithms can be adopted for emergency situations, while location retrieval might be used for reporting incidents, providing custom tailored offers or discounts based on identified patterns.

In the context of the Covid-19 pandemic, Google and Apple joined forces to create a built-in software solution for Android and iOS that could notify mobile phone owners if they were exposed to positive patients. Their initiative is suitable for both outdoor and indoor scenarios grace to the way the application is expected to be implemented and the technology it relies on. Firstly, the purpose of the application is to keep a record of the encounters within two meters the owner had in past two weeks, rather than precisely estimating the location. Secondly, the Bluetooth technology intended to be used for identification behaves well for short distances where usually no obstacles interfere. Once the system will be deployed, mobile phones will be able to exchange encrypted unique codes using Bluetooth radio signals with other peer devices located in proximity. The history of these exchanges is persisted only for fourteen days. In the meantime, if one person is diagnosed with Covid-19 the infrastructure would be able to identify the phones that were in close adjacency and inform the owners they have potentially been exposed [20]. Besides the importance of this joint project, the academia and security experts challenged the initiative for data protection and privacy. Many questioned the possibility of external parties to interfere with this communication protocol and acquire data about the subjects without their consent.

Among other techniques, indoor positioning represents a valuable source of information about an individual. Studying someone's daily routines in respect with a reference setup can reveal details about subject's personality in a similar extent with social media activity monitoring. For example, if the reference setup is a supermarket where the subject uses to go weekly for shopping, a real time tracking system could estimate whether the person is passionate by technology, by reading, whether the person lives in a house or an apartment, whether the person has children or owns a pet, whether the person follows a healthy diet, or rather frequents the sweets shelves and uses to drink alcoholic beverages. An analysis of the actual areas within the supermarket where the subject spends most of the time might reveal some food habits - whether someone prefers natural, unprocessed, or canned, convenience food. Such information correlated with the hours when someone usually comes for shopping and the average length of the visits can describe either a morning person or an individual with a busy schedule. A research from the University of Ulster "modeled human movement patterns by applying a discrete Bayesian filter to predict the areas that will, or will not, be visited in the future" using Wi-Fi signals [21].

In addition, many applications nowadays allow users to register using already existing accounts on social media platforms like Facebook, Google, Twitter or Instagram. What few people understand is by connecting with social media accounts on different websites, the companies owning the social platforms get access to other activities that are not normally related to their scope. When surfing the Internet for news, users end up with multiple social media trackers recording what they are doing on that website, what articles they are reading, and which ones get their attention. Therefore, indoor positioning systems architects should carefully reflect on the possible consequences when designing a service. On the one hand, from a user engagement perspective, an application that allows users register with a different account is more convenient since they do not have to remember new credentials, they are not requested to fill in registration forms and just a simple social authentication will let them access the application. On the other hand, when privacy is exchanged for convenience, different third parties might start collecting personal indoor positioning data.

IV. DATA PRIVACY IN ONLINE SOCIAL NETWORKS

Besides the many benefits it offers, such as keeping in touch with people, distributing multimedia content or viewing the latest news, social networks bring various concerns regarding data confidentiality, which can have financial, psychological, or reputational consequences.

Some of the most common deterrents revealed on social networks include identity theft, cyberstalking, sexual harassment, child abuse. Especially, these dangers target vulnerable people that use social networks, who usually fall under certain typologies, representing individuals that are the most prone to act according to the attackers' interests. Also, actions such as negative publicity, online victimization among the minors or online stalking of candidates for job interviews on social media platforms can lead to changes in individual behavior and restrain the right to free speech.

For proper data security and integrity within social networks, there are several suggestions that must be followed by the owners of social network accounts or other probably concerned people (for example, parents, caregivers, etc.). In this sense, clear understanding about privacy policies, keeping account information private, accepting only valid friend requests, and turning off location sensors when they are not required are just a few that can be listed. Knowing the privacy policies is important because social networks have their own policies and every user should consider what personal data will be processed, as well as any further connection between the social media account and other third parties. Also, the creation of user accounts usually involves the distribution of personal information such as biographical data, interests and passions, political orientation, religion, bank account details or personal numerical code; if this information becomes available to cybercriminals, it can be used for fraudulent purposes. Similarly, a best practice is to accept friend requests only from known people, since behind some friend requests can hide dangerous attackers who can take advantage of vulnerable people. Last, but not least, another suggestion is to turn off location sensors when they are not needed, thus avoiding various requests from applications for frequently visited locations that could end up tracking activity.

Within social networks there are numerous algorithms based on artificial intelligence and machine learning that help creating user's profile. These algorithms require data on the activities within a particular user's network. User profiling is based on data recorded by the platform in question; a complex analysis of all activities on all platforms involves the aggregation of all data and, implicitly, the distribution of this information to a third party.

In "An Overview on User Profiling in Online Social Networks" [22] the authors present a series of steps that are completed in a user profiling process. Thus, after registering the data within the social network, the activities, the images and the location are extracted. These steps are followed by identifying a pattern of actions performed by user, detecting faces in images, analyzing the meaning of the text and the friends' network. An aggregation of those extractions provides a behavioral analysis of the individual, known in specialty literature as social profiling.

In the digital age when personal information is stored on various platforms, it has become necessary to define the right of any individual "to be forgotten". In this regard, once this right is granted by the European Court of Justice by defining the General Data Protection Regulation (GDPR), any person interested in deleting personal data may request this from the company that holds the information, for any reason [23]. The definition of the right "to be forgotten" include images, videos, articles or other materials about the person in question, which can be found online. Consequently, any content that is found by search engines stays under the protection of the General Data Protection Regulation (GDPR).

Positive perspectives of the "right to be forgotten" may refer to information that is no longer relevant for the purpose of their collection, withdrawal of consent for personal data processing, unauthorized data harvest in marketing campaigns or illegal processing and are brought by a law that requires data deletion, especially for those which belong to a minor [24]. Most of the time, the details that are subject to these requests may seriously affect the personal or profession life and can influence the perception of other individuals.

V. ONLINE PAYMENTS

As mentioned above, maintaining confidentiality and data protection is becoming a real challenge in the age of technology. Thus, new changes are needed on the regulatory side to keep pace with both technological developments and cyber security threats; in this way, the risks of unauthorized access to data and their processing are minimized.

European regulations in the field of electronic payments have been established to assure data confidentiality through various mechanisms. These regulations are segmented on certain payment market areas and include the General Data Protection Regulation (GDPR), the Payment Services Directive (PSD2) or the Payment Card Industry Security Standards Council (PCI SSC). By assessing them, it can be stated that GDPR balances people rights regarding personal information and defines obligations for data controllers and processors, PSD2 creates a favorable development environment for payments service providers - PSPs on a market with a banking monopoly and assures strict validations in terms of security and integrity for banking operations, also targeting third-party electronic services, which can access account information via the Internet as a result of a consensus, with a major impact on the growth of e-commerce services. PCI SSC involves a definition of contractual relationship between parties involved in card payments and how card and sensitive authentication data can be secured so that the risks of security breaches are significantly reduced. According to PCI SSC, cardholder information includes a Primary Account Number (PAN), cardholder name, expiration data and service code. Also, sensitive authentication data contains details stored on magnetic card or chip, CAV2 / CVC2 / CVV2 / CID, as well as and PIN.

An interesting overview regarding electronic payments has been exposed in "Loss of privacy in electronic payment systems" [25]. From the authors' point of view, users do not realize the importance of privacy data in electronic payment systems until they lose this right. Often, many users believe that data privacy is an obstacle in developing safer and more efficient systems. For example, if a customer provides more personal information and the payment network detects unusual transfers within the account, this may require additional confirmation. This case also involves permanent monitoring of the client's location, as well as the analysis of payments and recipient accounts.

In payments case, the cash disappearance and the continuous increase in number and value of transactions made through electronic payment engines can influence the destabilization of the economy. The payment systems regulated by the states would allow the control of the economic life. For example, the funds of individuals or companies could be blocked for various reasons much more easily and the power to make decisions could lead to various abuses. By analyzing people's habits, a large part of the population is not yet ready for cash disappearance.

Regarding digital payments, there are various examples that can compromise the data protection activity. By integrating its own digital wallet into instant messaging services such as Facebook Messenger or WhatsApp, Facebook can once again become the target of new charges by associating financial information with users' personal information. In this way, Facebook can take advantage of access to financial and personal information by monetizing them, which is a real danger for every individual [26].

VI. CONCLUSIONS

Following the amplitude of prior data driven manipulation campaigns and foreseeing the challenges the future may lie down, the United States subsidiary of the Institute of Electrical and Electronics Engineers adopted a statement in 2018 for digital personal privacy, awareness and control [27]. The statement recommends a shift in the way software applications are currently designed. For the better, service providers ought to place the user at the core of their business. In a metaphorical way, companies should follow the principles Simon Sinek evoked in his book "Start with why" [28]. Their business activities have to be motivated by purposes that address real needs, not primary by profits. Profits should be the consequence, not the reason. For achieving this goal, software applications providers must assure complete disclosure for users regarding all the information that is directly or indirectly collected by the service itself or by any other third party involved. The users must always have control over their own personal data; it should be the standard to know who is collecting the data, what kind of data is collected, where that information is stored, for how long and for what purposes. Technology companies should adhere to public transparency regarding users' data. The latter have to know what collection techniques are used to track activity and harvest data, from less-conspicuous trackers like local shared object Flash cookies and browser fingerprinting to web beacons, scripts, tracking images or ads. Users' decision to not allow services track them should be extended to any entity involved, including third parties and service providers. Of course, explicit requests asking for data deletion should be respected and legal disputes resulting from refusing to comply must not be restricted by favorable laws or circumstances. Security incidents that result into personal data loss must never remain unknown to the users and the entities that infringed policies and the mechanisms they applied should be disclosed. Nevertheless, users' notification whenever they are exposed to paid contents, associated with information about the origin of the content and the deliberate beneficiary, would represent a best practice. Equally, the sponsors identity could be disclosed in websites metadata as a form of transparency that lets users get a broader understanding about the information they are consuming and judge wittingly.

The future of technology is probably going to orient itself towards decentralization. This movement provides solutions for currently stringent security issues and initiatives where privacy is the default start emerging. Actions that align users, developers, and publishers, providing the first group control over his own social graph and preventing companies from being responsible for vast amount of information shall be encouraged and expanded.

The prospect towards the society aspires should be an ethical one, where public institutions impose regulations that protect individuals from being iniquitous exploited without both their consent and full understanding, while companies serve moral customer needs.

REFERENCES

[1.] PM Greenfield. Technology and Informal Education: What Is Taught, What Is Learned. *Science*, 2009, 323(5910). https://doi.org/10.1126/science.1167190
[2.] Your Outboard Brain Knows All. Available at: https://www.wired.com/2007/09/st-thompson-3/, accessed in December 2021.
[3.] NG Carr. *The shallows: What the Internet is doing to our brains*. W. W. Norton & Company, New York, 2010.
[4.] S Krach, FM Paulus, M Bodden, T Kircher. The rewarding nature of social interactions. *Frontiers in behavioral neuroscience*, 2010, 4(22). https://doi.org/10.3389/fnbeh.2010.00022
[5.] Harvard Medicine magazine: Trust Me, I'm Your Smartphone. Available at: https://hms.harvard.edu/magazine/connections/trust-me-im-your-smartphone, accessed December 2021.
[6.] JA Obar, A Oeldorf-Hirsch. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 2020, 23(1), p. 128-147.
[7.] G Bolsover, P Howard, P. Computational Propaganda and Political Big Data: Moving toward a More Critical Research Agenda. *Big Data*, 2017, 5(4), p. 273-276.
[8.] Bloomberg: Cruz-Connected Data Miner Aims to Get Inside U.S. Voters' Heads. Available at: https://www.bloomberg.com/news/features/2015-11-

12/is-the-republican-party-s-killer-data-app-for-real-, accessed December 2021.
[9.] W Youyou, M Kosinski, D Stillwell. Computer-based personality judgments are more accurate than those made by humans. *In:* Proceedings of the National Academy of Sciences, 2016, 112(4), p. 1036-1040.
[10.] C Wylie. Mindf*ck Cambridge Analytica and the Plot to Break America. Penguin Random House, New York, 2019.
[11.] The #Election2016 Micro-Propaganda Machine. Available at: https://medium.com/@d1gi/the-election2016-micro-propaganda-machine-383449cc1fba, accessed December 2021.
[12.] #Election2016: Propaganda-lytics & Weaponized Shadow Tracking. Available at: https://medium.com/@d1gi/election2016-propaganda-lytics-weaponized-shadow-trackers-a6c9281f5ef9, accessed December 2021.
[13.] FakeTube: AI-Generated News on YouTube. Available at: https://medium.com/@d1gi/faketube-ai-generated-news-on-youtube-233ad46849f9, accessed December 2021.
[14.] V Chotpitayasun, K Douglas. How "phubbing" becomes the norm: The antecedents and consequences of snubbing via smartphone. *Computers in Human Behavior*, 2016, 63, p. 9-18
[15.] The Cost of Cybercrime Study – Ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection. Available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50, accessed December 2021.
[16.] The Economist: The world's most valuable resource is no longer oil, but data. Available at: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, accessed December 2021.
[17.] Indoor Positioning and Navigation System Market, by Component (Hardware, Software), by Technology (UWB, Bluetooth Low Energy, RFID, Cellular, WLAN) by Platform (Android Based, iOS Based), Forecast to 2027. Available at: https://www.marketresearchfuture.com/reports/indoor-positioning-navigation-system-market-1775, accessed December 2021.
[18.] E Jeong, B Seo, N Kim, D You, D Kim, Y Lee. An indoor positioning method in a concert hall using optical camera communication (OCC) technology. *In:* International Conference on Information and Communication Technology Convergence (ICTC). Jeju, 2017, p. 970-972
[19.] J Huang, Z Huang, K Chen. Combining low-cost Inertial Measurement Unit (IMU) and deep learning algorithm for predicting vehicle attitude. *In:* IEEE Conference on Dependable and Secure Computing. Taipei, 2017, p. 237-239.
[20.] Google and Apple Reveal How Covid-19 Alert Apps Might Look. Available at: https://www.wired.com/story/apple-google-covid-19-contact-tracing-interface, accessed December 2021.
[21.] E Furey, K Curran, P Mc Kevitt. HABITS: A Bayesian Filter Approach to Indoor Tracking and Location. *International Journal of Bio-Inspired Computation*, 2012, 4, p. 79-88.
[22.] G Vasanthakumar, K Sunithamma, P Deepa Shenoy, K Venugopal. An Overview on User Profiling in Online Social Networks. *International Journal of Applied Information Systems (IJAIS)*, 2017, 11(8), p. 25-42.
[23.] F Fabbrini. E Celeste. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, 2020, 21(S1), p. 55-65.
[24.] What is the Right to be forgotten? Available at: https://www.igniyte.co.uk/personal-reputation-management/right-to-be-forgotten/, accessed December 2021.
[25.] A Vasić, N Tomić. Loss of privacy in electronic payment systems. *The Annals of the Faculty of Economics in Subotic*, 2020, 56(43). https://doi.org/10.5937/AnEkSub2001135P.
[26.] How to Protect Your Privacy on Social Media? Available at: https://dataprivacymanager.net/how-to-protect-your-privacy-on-social-media/, accessed December 2021.
[27.] Digital Personal Privacy, Awareness and Control. Available at: https://ieeeusa.org/assets/public-policy/positions/security/DigitalPrivacy0618.pdf, accessed December 2021.
[28.] S Sinek. Start with Why: How Great Leaders Inspire Everyone to Take Action. Penguin, London.