GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-based Approach

Javed Ahmed, Sule Yildirim, Mariusz Nowostaki, Raghvendra Ramachandra, Ogerta Elezaj and Mohamad Abomohara
Norwegian University of Science and Technology
Gjøvik, Norway
Email: {javed.ahmed, sule.yildirim, mariusz.nowostawski, raghavendra.ramachandra, ogerta.elezaj, mohamed.abomhara }@ntnu.no

***Abstract*—The enforcement of the General Data Protection Regulation (GDPR) represents a great challenge for online social networks (OSNs). Several OSNs are making significant changes to their systems to achieve compliance with GDPR. OSNs are required to obtain meaningful consent from users to achieve GDPR compliance. GDPR recognizes user's consent as a legitimate ground for personal data processing in the context of online social networks. This article presents a comparative study about the criteria for valid consent under GDPR and existing consent seeking practices of OSNs. In order to simplify the comparative process, Facebook is taken as a case study for online social networks. In conclusion of the comparative study, we argue that existing consent mechanisms in OSNs are not GDPR compliant. To achieve GDPR compliance in online social networks, we advocate a blockchain-based approach for consent management. This paper paves the way for designing a blockchain-based GDPR compliant consent management model for personal data processing in online social networks.**

Keywords-Blockchain; GDPR; Online Social Networks; Compliance; Data Protection.

I. Introduction

Online social networks become a social data hub on the Internet. They collect a massive amount of personal and sensitive data from the users. Since its inception, Facebook collected 300 petabytes of personal data which is increasing at the speed of 4 new petabytes per day [15]. Data has become an enormously valuable asset in our economy today. It is commonly considered as the oil of the 21st century, which is not only fueling the success of the tech giants (i.e. Facebook, Google, Youtube, Instagram) but also driving innovation and economic growth. The current situation is that the benefits of data-driven society are reaped by only a few tech giants which make the majority of the profit through offering services for which users pay with their personal data. Users have little or no control over their personal data that is how it is used and where it is stored. In recent years, mainstream media has repeatedly covered controversial incidents related to abuse of personal data entrusted to online social networks [3], [7]. The recent Cambridge Analytica scandal raises serious concerns about technical, commercial, political and ethical aspects of personal data collection. The scandal brought up the fact that service providers exhibit enormous social influence that can shake or derail the democratic foundation of western societies.

The General Data Protection Regulation (GDPR) [17] aims to empower data subject by giving control of personal data back to them. GDPR imposes a certain set of data protection requirements on data controllers and processors to achieve this goal. These requirements not only offer more control over personal data but also enable transparency in data processing activities carried out by the controllers and processors. Online social networks face a great challenge from legal and technical perspectives due to the enforcement of GDPR [8]. Online social networks are not fully prepared to comply, and when they try, they often have major gaps in compliance with the regulations. In the context of online social networks only legitimate ground to process personal data of the users is by seeking explicit consent from the data subject. The main aim of promoting the notion of consent is to provide data subject control over their personal data. At present, consent management mechanisms in OSNs are either non-existent or not GDPR compliant [4]. In the absence of such a mechanism, data subjects face a lack of control over their personal data which in turn gives rise to privacy breach scandals such as Cambridge Analytica. GDPR compliance is thus the only way to empower data subjects and make data controllers and processors accountable.

We have conducted a comparative study to analyze the current status of consent mechanisms in online social networks with reference to criteria for valid consent under GDPR. In order to simplify the comparative process, we have taken Facebook as a case study. Facebook is one of the most widely used online social networks which represents the user base of more than 2 billions. Therefore, Facebook can be considered as an adequate case for representing online social networks. The findings reveal that consent given to online social networks is implicit, non-informed, not freely given and bundled for multiple purposes. Whereas, valid consent under GDPR must be explicit, informed, freely given and specific to a single purpose. This issue of non-compliance opens up new research direction and pose interesting research challenges.

978-1-7281-7283-5/20/$31.00 ©2020 IEEE
DOI 10.1109/ICICT50521.2020.00054

We address this issue of non-compliance in our research and identify that personal data processing and sharing activities carried out by online social networks lack transparency. In order to enable data controllers and processors to comply with GDPR require transparency in data processing activities. The existing research reveals that transparency is a key component in achieving privacy and compliance [14]. Transparency is the key characteristic of blockchain technology that can add value to the consent management mechanism for personal data processing. A blockchain-based approach can provide greater transparency to OSN users regarding their personal data. Each user can have complete transparency over what data is being collected about him/her and how it is accessed. Blockchain also asserts data ownership and user privacy by enabling transparency. At the same time, blockchain provides anonymity to its users by allowing them to create pseudo-anonymous transactions without the need for revealing personally identifiable information about them. A blockchain-based consent management mechanism can be designed to address the aforementioned issues of non-compliance and privacy.

The rest of the article is organized as follows. In section 2, we present a conceptual model of informed consent along with criteria for valid consent under GDPR. In section 3, we present the findings of a comparative case study. In section 4, we discuss the status quo of the consent management mechanism and propose alternative options to design the GDPR compliant consent management model. Finally, we conclude the paper with future research directions and open research problems.

II. Consent Driven Data Protection

The notion of consent has been studied in multiple disciplines including medicine, law, moral philosophy, social and behavioral sciences. Consent is a multifaceted concept that strongly relies on the principle of autonomy. Self-determination and the concept of control form the basis for the principle of autonomy. Consent is the permission or agreement specified by the data subject for actions involving their personal data. The notion has been extended to web-based contexts, which means that consent usually has to be given to the terms of service of a website which provides legitimate grounds for a company to collect and process users' personal data. The notion of consent is quite diverse in nature and it has various forms. One such form is informed consent that is given by data subject upon clear realization and understanding of the facts, implications, and consequences of an action. The data subject acknowledges that he/she has been sufficiently informed of what the data is being used for and by whom. The main aim of promoting the concept of consent is to provide transparency and more control over personal data to the data subject.

Consent is also a key feature of GDPR regulation. GDPR aims to make consent more unambiguous and explicit. To demonstrate GDPR compliance is applicable to all organizations involved in the collection and processing of personal data. Online social networks collect large amounts of personal data about their users and fall under the scope of GDPR. Thus, the only way to achieve compliance is by obtaining the necessary consent from the data subjects. Therefore, consent is an important notion in online social networks, since it is based on the idea that individual online social networks' user make conscious, rational, and autonomous choices about the disclosure of their personal data. Whether they are always capable of making such choices and willing to do so in practice is dubious. There is mounting evidence that data subjects do not fully realize the consequences and risks associated with personal data disclosure. Below, we describe the current consent practices in the most widely used online social networks. Prior to that discussion following subsections present a conceptual model of informed consent and the main characteristics of a valid consent under GDPR.

A. Conceptual Model of Informed Consent

It is important to seek a clear understanding of what constitutes informed consent and how it can be realized in online social networks. Here, we provide a conceptual model of informed consent and discuss whether it is realized in existing online social networks or not. The conceptual model of informed consent was first developed by Friedman et al. [6]. It has been specifically designed in the context of online interactions. The model focuses on the ethical principle of autonomy and the concept of competence. These concepts refer to autonomous authorization and the data subject's competence to make the consent decision. The model is based on six conceptual components as depicted in Figure 1. These conceptual components are disclosure, comprehension, voluntariness, competence, agreement, and minimal distraction. The term informed consent is significant in its meaning. The word informed encompasses disclosure and comprehension. The word consent encompasses voluntariness, competence, and agreement. Minimal distraction refers to the activity of giving consent without diverting data subject from their primary task.

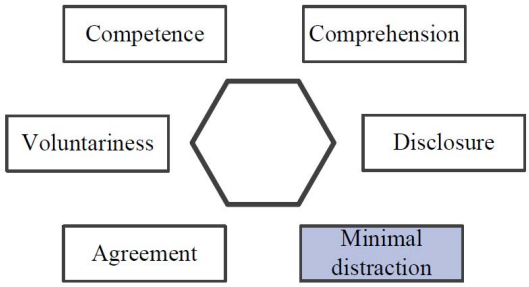

Fig. 1. Conceptual Model of Informed Consent [2].

Disclosure deals with the data subject's understanding of benefits and potential harm that might be expected by consenting to personal data processing activities of the service provider. A data subject should be able to understand accurately the privacy policy to which he/she is agreeing while

giving consent. Comprehension deals with the data subject's accurate interpretation of what is being disclosed. However, it is not possible to guarantee that all data subjects will completely understand all aspects of consent. Voluntariness refers to ensuring that the action is not controlled or coerced and the data subject is not forced or manipulated to give consent. Competence refers to possessing the mental and physical capabilities needed to be capable of giving consent. A data subject who lacks those competencies needs to have their representative to give consent. This is because they cannot reliably determine the appropriateness of the information they choose to disclose. Agreement refers to a reasonably clear opportunity given to data subject to accept or decline the consent. Moreover, it means that data subject can choose among different options without losing the right to service. Minimal distraction refers to giving consent without unduly diverting data subjects from their primary task. The process of obtaining consent necessarily disengages data subject from the task at hand, but the activity should not entirely divert users from their current actions.

We analyze the status of online social networks in light of the aforementioned discussion about the conceptual model of informed consent. Disclosure requires informing data subjects about the goals of data processing. It is an important aspect to discuss how this information is presented by online social networks. Most of the OSNs present this information via a privacy policy. Comprehension requires data subjects' accurate interpretation of these privacy policies. It has been demonstrated that data subjects do not read privacy policies and even if they did, they probably would not be able to entirely understand it. A data subject should not be forced or manipulated to give consent under the voluntariness aspect of the conceptual model. The users are tempted to give consent to online social networks in order to get free service. Therefore, consent given to OSNs is provided through Hobson's choice which means that either data subjects entirely accept privacy policies or they are not allowed to be part of the online social network. Thus, the consent is not truly given voluntarily.

Online social networks are complex, interwoven and ubiquitous services that facilitate many kinds of online interactions such as data subject to service provider interactions, data subject to third party interactions, and data subject to data subject interactions. It is difficult to determine when one context ends and a new one begins. The users are not able to contemplate fully the consequences and risk of personal data processing due to the complex and ubiquitous nature of OSNs. Therefore, we argue that they lack the required competence to see through the lens of privacy policy risks associated with disclosure of personal data. As discussed earlier, widespread consent seeking practice in online social networks is Hobson's choice which forces data subjects into all or nothing options. It is in clear violation of the agreement component of the conceptual model. Most of the online social networks comply with the minimal distraction policy and do not disengage users from the core task of socialization while seeking users' consent. We present a comparative analysis of various components of the conceptual model with current online social networks in the table 1.

TABLE I
COMPARISON OF ONLINE SOCIAL NETWORKS WITH CONCEPTUAL MODEL

OSN Platforms	Disclosure	Comprehension	Voluntariness	Competence	Agreement	Minimal Distraction
Facebook	✓	✗	✗	✗	✗	✓
Google+	✓	✗	✗	✗	✗	✓
LinkedIn	✓	✗	✗	✗	✗	✓
Instagram	✓	✗	✗	✗	✗	✓

B. Criteria for Valid Consent Under GDPR

With the enforcement of GDPR, the data controllers and processors handling EU citizens' personal data must ensure that they are compliant with the new data protection requirements of GDPR. Online social networks have a considerable amount of user base within the European Union. There has to be some legal basis in order to collect and process personal data of EU citizens. GDPR identifies six lawful bases for the processing of personal data. Obtaining meaningful user consent is the only applicable legal basis for online social networks to collect and process personal data of the EU citizens. Consent can only be an appropriate legal basis if the user is offered control and a choice with respect to accepting or declining the terms offered without any negative consequences. Under GDPR consent is considered to be valid only when it has certain characteristics that include freely given, informed, specific and unambiguous (explicit). A brief description of these characteristics is as follows:

1) **Freely Given:** It means that data subject must be able to exercise real choice without being forced or coerced while giving consent. Consent is not freely given if there is a clear imbalance of power between controller and data subject or data subject has no genuine and free choice or is unable to deny or withdraw consent easily. Another important attribute of the freely given consent is that data subject should not be facing negative consequences if he/she decides not to given consent.
2) **Informed:** Informed consent deals with enabling data subject to understand what they are consenting to, therefore, consent must be taken by informing the nature of processing in an intelligible format with a minimal set of prose. It is within the scope of the informed characteristic that data subject should fully understand what are the implications of their action.
3) **Specific:** Specificity of consent promotes transparency therefore data controller must seek consent separately for each purpose of data processing. It increases data subject's control over his personal data.
4) **Unambiguous:** The unambiguous feature of consent is tied to the fact that it must be explicit. Explicit consent requires data subject to take clear affirmative action as an indication of acceptance to the proposed processing of personal data. Therefore, inactivity, failure to opt-out and pre-ticketed opt-in boxes do not form valid consent under GDPR.

Apart from these characteristics, GDPR also provides a data subject with the right to withdraw their consent at any time. Thus, a data controller should provide a mechanism to withdraw consent easily. General structure of consent may comprise of three components which include consent form filled by data subject, context of the consent which usually contains data about time, location and relevant information communicated between data controller and data subject, and details of permission set by data subject such as permitted and prohibited actions, allowed party, validity period, etc. Consent goes through different phases in its lifecycle. Fatema et al. [5] identified seven phases of the consent lifecycle: collection, storage, process, modification, revocation, archive, and destruction. Initially, consent is collected, then stored and processed for checking compliance with data processing. According to GDPR, data subject can modify consent that is equivalent to revoking the previous consent and giving a new one. Any changes to consent need to be archived for the duration necessary for compliance or provenance purposes before finally it is destroyed. The existing research literature reveals that there remains a gap between OSNs users' understanding of consent and subsequent data usage by OSN service providers. One of the main reasons for the lack of understanding associated with the consent process is the length of the policy document and the complex language used. In the following section, We will evaluate the consent culture in online social networks with reference to criteria for valid consent under GDPR.

III. Non-Informed Consent Culture in OSNs

Consent becomes an important notion in online social networks due to the enforcement of GDPR. The consent provides an opportunity for individual OSN users to take a conscious, rational, and autonomous decision about the disclosure of their personal data. The important question is whether online social network users are always competent to take this decision and disclose their personal data willingly. There is mounting evidence that OSN users do not fully contemplate the consequences and risks of personal data disclosure. The users without any technical knowledge (even with technical knowledge) are not capable to see through the data processing in social media. Most of the users are unaware of data collection and processing rules [1]. Individual social media users have to deliver data in return for socialization. Online social network users consider data disclosure as a part of the deal that they have made with OSNs in exchange for gratis services. The consent culture of social media has turned into blanket non-informed consent culture and users accept this through a click on the accept-button in their end-user license agreements (EULAs) that sites seek from their users upon sign-up. As per the current statistics from EU countries, most of the OSN users do not read these end-user license agreements [1]. The research proves that privacy policies are far too complicated for ordinary users to comprehend and social media users can't turn down privacy policies [11], [12]. Moreover, these privacy policies have a minimum impact on personal data disclosure practices. Online social networks and third-party applications collect more data than necessary that is in contradiction with the data minimization principle of GDPR. We argue that consent in social networks is predicated on a type of uninformed consent that has the effect of disempowering data subjects over the information held about them.

A. Analysis of Consent Given to OSNs

GDPR compliance requires a data controller to obtain meaningful and valid consent from the data subject. In this section, we analyze the present status of consent in online social networks in the light of the discussion in section II.B about criteria for valid consent as per GDPR. We take Facebook as a case study in order to simplify the analysis of online consent. Facebook can be considered as an adequate case study because of its popularity and user base. Facebook is a leading online social network that has been questioned over the years by regulators about its privacy practices. Thus, we shall analyze what kind of consent users are giving to Facebook. Figure 1 shows the sign-up page for users who wish to join the Facebook community. The process of joining Facebook is easy and fast, on the one hand, fields to fill out are big and clear to see, on the other hand, the information regarding automatically agreeing to their terms of services, data policy, and cookie use policy is presented with a tiny font that does not grab attention. Moreover, when signing up for the service, data subjects are just given an opportunity to click on the links redirecting them to the term of service, data policy and cookie use policy pages. It has been proved by the research that users do not read terms of service even when they are specifically asked to do so. In the case of Facebook, potential users are being told where they can find the information concerning what they are agreeing to. It is very unlikely that users will spend time to analyze what they are accepting [13].

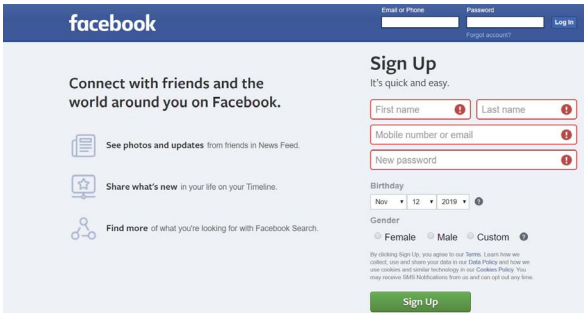

Fig. 2. Facebook sign up page.

It is not yet clear what kind of consent users are giving to Facebook. Let us analyze the Facebook consent mechanism as per the characteristics identified by GDPR for valid consent described in section II.B. One of the important characteristics of valid consent under GDPR is that it should be freely given. As per the scenario outlined above, when users are joining Facebook, they have no choice but to consent to its terms

of service, data policy, and cookie use policy. Referring to the aforementioned scenario, somehow users are forced to give consent when entering the Facebook community. As per freely given consent, the data subject should not face negative consequences if he/she decides not to give consent. However, in the case of Facebook, it is not possible to join the community without agreeing to all terms of service, data policy, and cookie use policy. According to GDPR, refusal of consent must not be detrimental to the user, whereas, Facebook does not abide by this condition. In current settings of Facebook, users are asked to give consent for several purposes bundled together then it is not freely given consent as the data subject has to accept all purposes even if he/she finds only one of them acceptable. Apart from this, there is a clear imbalance of power between user and service provider, therefore, consent given to Facebook does not qualify as freely given consent.

According to GDPR, consent should be informed in nature which enables data subject to comprehend what they are consenting to. Consent given to Facebook is non-informed in nature due to several reasons. The first and foremost reason is that Facebook fails to provide information about terms of service in an intelligible format with a minimal set of prose. It is not sufficient to make this information available somewhere and give users the opportunity to click on the link redirecting them to these pages (refer to Figure 1). And even if users navigate to these pages and read, they probably would not be able to entirely understand it [16]. Secondly, informed consent promotes transparency which means users should know about the nature of data processing, whereas Facebook lacks transparency related to their data processing activities and users are unable to understand privacy risk related to their personal data disclosure. Thus, consent given to Facebook does not qualify as informed consent as per GDPR.

Specificity is another important characteristic of consent under GDPR which requires data controllers to seek consent separately for each purpose of data processing. Thus, provides data subjects fine-grained control over their personal data disclosure. A user wishing to join the Facebook community will be presented with a sign-up page shown in figure 1 that requires a bundled consent for multiple purposes. Apart from this sign-up example, there many Facebook features that require users to give bundled consent to the service provider. One such example is Facebook's facial recognition feature. This feature seeks bundle consent and does not allow users to give specific consent. Therefore, consent given to Facebook does not qualify as specific consent under GDPR.

GDPR requires explicit consent from the data subject which means consent must be given in clear affirmative action. In the case of Facebook, consent is automatically given by joining the community. The activity of joining Facebook would not be considered enough to make consent explicit. The explicit consent must be confirmed in clear affirmative action such as while joining the Facebook community potential users required to tick a box to express their consent. Apart from these attributes, GDPR provides the data subject with the right to withdraw consent at any time. Apparently, Facebook fails to provide any such mechanism to withdraw consent. We evaluated the existing consent mechanism on Facebook in light of GDPR's definition of consent. Current settings of Facebook by and large lagging behind to meet these GDPR requirements.

IV. Discussion

We have analyzed that consent given to Facebook is not GDPR compliant consent. It is important to discuss what kind of consent it is and how the GDPR compliant consent mechanism can be designed for online social networks. Tacit consent is one of the important notions in the history of political science. The term was coined by John Locke. According to the tacit consent doctrine, consent does not have to be expressed to be considered valid. The individuals give consent to governments simply by living in the territory in which that government operates [9]. The concept of tacit consent resembles the kind of consent data subjects are giving to online social networks. The concept of tacit consent does not require to be informed, freely given and explicit. The tacit consent does not require the citizen to be informed about their government's policy. Thus, this consent is not informed in nature. An individual has no choice in deciding his place of birth. He is automatically inserted into a certain social context that shapes his life according to it. Therefore, this consent is not freely given, as it does not derive from conscious and free choice. Finally, tacit consent is not explicit in nature because individuals do not have to express it in order to give consent to the state.

According to Santarelli, consent given to online social networks can be defined as tacit online consent [13]. The consent is given to online social networks simply by using their website. We compared tacit consent with the consent given to Facebook (tacit online consent) in the aforementioned discussion and observed similarities between the two. However, there are substantial differences between state and OSNs. The states exist for the welfare of the citizens, whereas, OSNs exist mainly for making some profit. Another crucial difference is that when consent is given to a state, an individual's privacy is not compromised. However, consenting to OSNs undermine an individual's privacy.

It has been demonstrated before that consent given to online social networks is far from being GDPR compliant. The important question is how to design a consent mechanism that would comply with the requirements of recent EU regulations. A consent management mechanism can comply with the requirements of GDPR by enhancing the transparency, auditability and data subjects' control over personal data. The main focus of the consent mechanism should be to regulate data flow from data subject to data controller and processor by controlling associated consent granted by the data subject. Blockchain technology can play a pivotal role in designing such a solution that maximizes the transparency of the data flow from data subject to the service provider and third parties. We owe an explanation to use blockchain technology for GDPR compliance, whereas the current research literature

suggests that two initiatives (GDPR and Blockchain) are at odds [10]. They seem to be at odds until we look at the underlying principles of GDPR and Blockchain. Both share common principles of data privacy and give data subject more control over their private data. Both GDPR and blockchain aspire to increase integrity, trust, and transparency in potentially hostile environments. The GDPR does so by imposing responsibilities upon data controllers and processors.

The GDPR assumes to an extent that data controllers and processors are centralized, law-abiding actors with control over the system. The GDPR compliance approaches based on centralized architecture result in limited transparency and lack of trust, among other things. It is also not clear how to align it with public blockchain systems for example. Blockchains ensure trust and transparency by utilizing the computational power of the masses and by sharing the ledger with all the peers in the P2P network. The unprecedented transparency provided by blockchain technology sits uneasily with GDPR obligations related to privacy and information confidentiality. The dilemma of adopting blockchain for consent management is to find the trade-off between transparency and information confidentiality. One of the solutions is to use private blockchain that allows only permitted parties to have access to all transactions. However, private blockchain loses the primary advantage of decentralization. Moreover, a dishonest central authority is capable of tampering the transaction history for personal gain. Wang et al. [18] propose a framework that preserves information confidentiality without compromising transparency using zero-knowledge proof. We conclude that prominent features of the blockchain technology can be effectively utilized to manage personal data fully complying with the GDPR legislation.

V. Conclusion and Future Work

We analyzed the existing consent seeking practices of online social networks and identified vulnerabilities that could potentially result in GDPR non-compliance. Our comparative study shows that GDPR requires informed, explicit, freely given and specific consent from the data subjects. Whereas, current consent seeking practices in OSNs are non-informed, implicit, not freely given (Hobson's choice) and bundled for several processing purposes. Additionally, we discussed that the privacy policies of OSNs are far from understanding of an ordinary user. It is not an easy task to exercise the user rights claimed in privacy policies. Furthermore, privacy policies do not meet the informed consent criteria of GDPR, even users with technical knowledge are unable to comprehend the data disclosure risks associated with agreeing to these policies. These privacy policies offer more room for improvement in order to meet the GDPR criteria of being intelligible and concise. It is evident from the existing practices that online social networks want to use the data subject's consent as a measure that merely legally transfers liability from the enterprise to the users.

In the future, we intend to develop a proof of concept prototype for blockchain-based GDPR compliant consent management model for online social networks. The main aim of developing this model is to offer data subjects more control over personal data processing, while at the same time enabling data controllers and processors to comply with consent and transparency obligations mandated by GDPR.

Acknowledgment

This work was carried out at the department of information security and communication technology, Norwegian University of Science and Technology, Gjovik, Norway during the tenure of an ERCIM 'Alain Bensoussan' Fellowship Programme.

References

[1] Anja Bechmann. Non-informed consent cultures: Privacy policies and app contracts on facebook. *Journal of Media Business Studies*, 11(1):21–38, 2014.

[2] Christian J Bonnici. An extended conceptual model of consent for information systems. In *Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems*, pages 149–154. IEEE, 2013.

[3] Ángel Cuevas, José González Cabañas, Aritz Arrate, and Rubén Cuevas. Does facebook use sensitive data for advertising purposes? worldwide analysis and gdpr impact. *arXiv preprint arXiv:1907.10672*, 2019.

[4] Sourya Joyee De and Abdessamad Imine. On consent in online social networks: Privacy impacts and research directions (short paper). In *International Conference on Risks and Security of Internet and Systems*, pages 128–135. Springer, 2018.

[5] Kaniz Fatema, Ensar Hadziselimovic, Harshvardhan J Pandit, Christophe Debruyne, Dave Lewis, and Declan O'Sullivan. Compliance through informed consent: Semantic based consent permission and data management model. In *PrivOn@ ISWC*, 2017.

[6] Batya Friedman, Edward Felten, and Lynette I Millett. Informed consent online: A conceptual model and design principles. *University of Washington Computer Science & Engineering Technical Report 00–12–2*, 8, 2000.

[7] Mike Isaac. Facebook security breach exposes accounts of 50 million users. 2018.

[8] Andreas Kotsios, Matteo Magnani, Davide Vega, Luca Rossi, and Irina Shklovski. An analysis of the consequences of the general data protection regulation on social network research. *ACM Transactions on Social Computing*, 2(3):1–22, 2019.

[9] John Locke. Second treatise on civil government. 1690. *Indianapolis, IN: Hackett*, 1990.

[10] Christopher Millard. Blockchain and law: Incompatible codes? *Computer Law & Security Review*, 34(4):843–846, 2018.

[11] Jayashree Mohan, Melissa Wasserman, and Vijay Chidambaram. Analyzing gdpr compliance through the lens of privacy policy. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, pages 82–95. Springer, 2019.

[12] Dijana Peras, Renata Mekovec, and Ruben Picek. Influence of gdpr on social networks used by omnichannel contact center. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1132–1137. IEEE, 2018.

[13] Maria Vittoria Santarelli. Locke's tacit consent in social networking sites: A case for tacit online consent. *The Information Systems Student Journal*, page 35, 2018.

[14] Oshani Seneviratne and Lalana Kagal. Enabling privacy through transparency. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, pages 121–128. IEEE, 2014.

[15] Kit Smith. 53 incredible facebook statistics and facts. 2019.

[16] Daniel J Solove. *Understanding privacy*, volume 173. Harvard university press Cambridge, MA, 2008.

[17] Paul Voigt and Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[18] Yunsen Wang and Alexander Kogan. Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30:1–18, 2018.