On Consent in Online Social Networks: Privacy Impacts and Research Directions

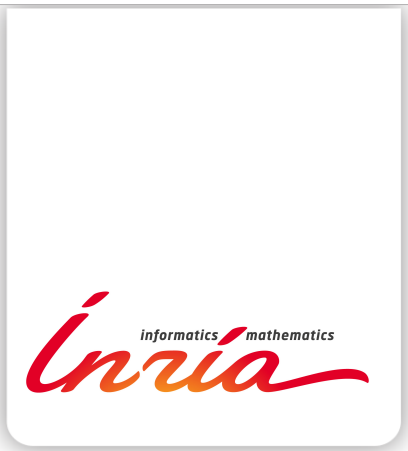
Sourya Joyee De, Abdessamad Imine

On Consent in Online Social Networks: Privacy Impacts and Research Directions

Sourya Joyee De, Abdessamad Imine

RESEARCH REPORT
N° 9197
Août 2018
Project-Team PESTO

ISSN 0249-6399 ISRN INRIA/RR--9197--FR+ENG



On Consent in Online Social Networks: Privacy Impacts and Research Directions

Sourya Joyee De, Abdessamad Imine

Project-Team PESTO

Research Report n° 9197 — Août 2018 — 8 pages

Abstract: The EU General Data Protection Regulation (GDPR) recognizes data subject's consent as a legitimate ground of data processing. At present, consent mechanisms in OSNs are either non-existent or not GDPR compliant. While the absence of consent means a lack of control of the OSN user (data subject) on his personal data, non-compliant consent mechanisms can give them a false sense of control, encouraging them to reveal more personal data than they would have otherwise. GDPR compliance is thus the only way to obtain meanigful consents, thereby protecting user privacy. In this paper, we discuss the characteristics of valid consent as per the GDPR, analyze the present status of consent in OSNs and propose some research directions to arrive at GDPR compliant consent models acceptable to users and OSN providers (data controller). We observe that evaluating privacy risks of consents to data processing activities can be an effective way to help users in their decision to give or refuse consents and hence is an important research direction.

Key-words: Online Social Networks (OSN), privacy, consent, GDPR, privacy risk

RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Le consentement dans les réseaux sociaux : Impacts sur la vie privée et axes de recherche

Résumé : En vigueur récemment dans l'Union Européenne, la Réglementation Générale de la Protection de Données (RGPD) stipule que le consentement d'un utilisateur est un préalable à tout traitement de données le concernant. Actuellement, les mécanismes de consentement dans les Réseaux Sociaux (RS) sont soit inexistants, soit non conformes à la RGPD. L'absence du consentement signifie clairement la perte de contrôle de l'utilisateur sur ses données personnelles. Quand le consentement est non conforme, il donne un faux-semblant de contrôle et encourage l'utilisateur à divulguer plus d'informations sensibles que nécessaire. La conformité à la RGPD est donc le seul moyen de manipuler des consentements clairs et contribuant à la protection de données personnelles. Dans ce rapport, nous discutons des caractéristiques du consentement valide selon la RGPD, nous analysons la conformité des consentements existants dans les RS et nous proposons des axes de recherche pour concevoir des modèles de consentement conformes et acceptables par les usagers et les fournisseurs des RS. Pour assister l'utilisateur à prendre les « bons » consentements aux différents traitements de données dans les RS, l'évaluation des risques sur la vie privée est un important axe de recherche.

Mots-clés : Réseaux sociaux en ligne, vie privée, consentement, RGPD, Risques sur la vie privée

1 Introduction

The EU General Data Protection Regulation (GDPR) [4], which has come into force across Europe from 25th May 2018, recognizes consent of data subject as a legitimate ground of data processing. The central aim of promoting the notion of consent is to provide data subjects control over their personal data.

Today, users reveal a wide variety of personal data in Online Social Networks (OSNs), not only to the OSN provider (the data controller) but also to third party applications and other users. OSNs involve a wide variety of data processing activities, such as face recognition and friend suggestion. At present, consent mechanisms for these processing activities are either non-existent or not GDPR compliant. This situation, in the absence of other legitimate reasons for data processing, is undesirable. The absence of consent means a lack of choice and consequently, a lack of control of the data subject on how his data is processed. Non-compliant consent mechanisms can give users a false sense of control, encouraging them to reveal more personal data than they would have otherwise [7]. Data controllers, third parties and/or governments may misuse the huge data repository accumulated by OSNs for surveillance, profiling leading various forms of discrimination and other privacy harms. Other malicious entities can misuse the data for identity theft, stalking, shaming, defamation and bullying, to say the least. On top of this, non-compliant data controllers are subject to hefty fines by the GDPR and may suffer loss of reputation among an increasingly privacy-conscious population when privacy harms come to light.

Quitting OSNs to protect one's privacy is not an effective measure. OSN providers can still possess the data of past members and collect information about non-users. Moreover, users derive various social benefits from OSNs, such as establishing new friendships and reviving and strengthening existing ones [2]. Therefore, the right approach to ensure user privacy is for data controllers to be compliant to privacy regulations and compliance of consent mechanisms constitute a major step in this direction. Achieving consent compliance is not an easy task in OSNs. In OSNs, often, user privacy depends both on the data subject's consent and other users' actions. Users face many cognitive and structural challenges in their decision to give or refuse consent [7]. Moreover, a compliant consent mechanism must have certain characteristics and to be practical, must be acceptable to both users and OSN providers. These issues open up new research directions to be explored. Privacy risk evaluation of consents for data processing activities can be an effective way to help users to decide whether to give or refuse consents and is an important research direction. The GDPR encourages informing users about the privacy risks of personal data processing.

In this paper, we first discuss what constitutes a "valid consent" according to the GDPR in Section 2 and then, in Section 3, we analyze the current state of consent in OSNs, with a focus on examples from Facebook, the leading OSN provider. Finally, in Section 4, we propose some research directions to arrive at GDPR compliant consent models acceptable to both OSN providers and users.

In the context of OSNs, users are the "*data subjects*", the OSN service provider is the "*data controller*" and third party application providers are the "*third parties*" as defined in the GDPR. We also use the terms "*personal data*" and "*data processing*" in the sense of the GDPR.

2 Valid Consent as in the GDPR

A valid consent, as in Article 4 of the GDPR, must be 1) freely given, 2) specific, 3) informed and 4) obtained by a clear affirmative action of the data subject. Below, we briefly describe these characteristics.

Freely given. The WP29 guideline on consent [1] describes how to assess whether a consent is indeed freely given using the following criteria: 1) the relationship between the data controller and the user, 2) the conditionality and 3) the granularity of the consent and 4) if the withdrawal of consent is detrimental for the user. It is unlikely that consent is freely given if there is a *power imbalance* between the data controller, such as an employer, and the data subject who may fear significant negative consequences if he does not give consent. If the performance of a contract is *conditional* on the consent to data processing not necessary for the execution of the contract, then consent is not freely given. If a data controller seeks the consent for several purposes bundled together, then it lacks *granularity* as the data subject does not have the freedom to give or deny consent for each purpose. Refusal or withdrawal of consent must not be *detrimental* to the user. If a user gives consent to Facebook's facial recognition feature meant for tag suggestions, detection of fake accounts etc., it is not "freely given" as the data subject has to accept all purposes even if he finds only one of them acceptable.
Specific. When several data processings have the same purpose, consent may be sought for all of them together. However, if a data processing has multiple purposes, then consent must be sought for each of them. Specificity of consent promotes transparency as the data subject knows about each purpose of data processing, increases his control over these purposes and safeguards against function creep. Facebook's facial recognition feature does not allow users to give "specific" consent as the provider does not ask for consent for each purpose.
Informed. To really enable data subjects to understand what they are consenting to and to exercise their rights, such as the *right to withdraw consent*, the data controller must provide, in plain and clear language, a minimal set of information including its own identity, the purposes of processing and the data that are to be collected and used. Informed consent thus promotes transparency.
Clear affirmative action. Data subjects must give consent in an active motion or declaration. Thus, opt-out and pre-ticked opt-in boxes in consent forms are invalid under GDPR. For example, Twitter requires users to uncheck pre-ticked boxes to opt-out of targetted advertising, making the resulting consent invalid. Silence, inactivity or simply proceeding with a service without any action are not consents.

3 Consent in Online Social Networks: Present Status

In OSNs, personal data is transferred from the data subject to the data controller (OSN provider), or third party application providers or other data subjects. These data transfers can be summarized into: 1) data subject-data controller interaction, 2) data subject-third party interaction and 3) data subject-data subject interaction. The last type of interaction is unique to OSNs. Several data processing activities can be related to each interaction and, according to the GDPR, all such activities require user consent to be legitimate. At present, such consent mechanisms in OSNs are either non-existent or if they exist, are mostly not GDPR compliant. In the following sub-sections, for each interaction, we discuss the current state of consent in OSNs. Facebook is a leading OSN provider, which has been questioned over the years by regulators and privacy advocates about its privacy practices [10]. It is yet to be seen how Facebook manages to comply with the GDPR. With this in mind, we focus mainly on Facebook for examples of consent mechanisms.

Data subject-data controller interaction. Targetted advertising, based on personal data available from user profiles and activities or from external sources, is the primary source of revenue for OSNs today. These advertising platforms can be exploited to cause privacy problems, such as inferring users' full phone numbers just from the knowledge of their e-mail addresses [11].

In response to the GDPR, Facebook has recently started seeking consent on whether to include data from its partners such as other websites to show advertisements, but it gives no options to users to say no to targetted advertisements. In contrast, Snapchat and Twitter have enabled their users to opt-out of targetted advertising [9]. However, opt-out and pre-ticked opt-in boxes in consent forms, under the GDPR, do not constitute valid consent.

Facebook's face recognition feature can be used to scan the profile picture and other photos and videos of a user to compute a template which can then be matched with other photos and videos in Facebook. It serves a few purposes: 1) suggest other users to tag the data subject in photos they have uploaded, 2) notify the data subject about photos and videos they appear in but have not been tagged, 3) detect fake profiles that use the data subject's photos and 4) identify people in photos they are not tagged in for people who use a screen reader. The current consent mechanism allows the user to give consent for all purposes or none at all, thus lacking in specificity and granularity. Users may be interested to enable the facial recognition feature for detecting fake profiles but not for photo tagging. So, refusal of consent leads to losing out on otherwise useful service(s) and hence is detrimental to the user.

Data subject-third party interaction. When using third party applications on the OSN platform, users often have little comprehension of how much data they are sharing, with whom and that they are also responsible for sharing their friends' information [6]. Recently, an app called "thisisyourdigitallife" was used to gather the personal data of its users and their friends in the disguise of a paid psychological test on Facebook. This data was then shared with Cambridge Analytica which may have used it to influence choices in elections. Such data sharing, without valid user consent, may lead to many harms like loss of jobs and insurance and suppression of free speech [5]. To use third party gaming applications on Facebook, users must agree to disclose personal data such as their public profile, name, e-mail address, date of birth, friend list etc., by clicking on a "Play Now" button. Although Facebook provides an explanation below this button that clicking it implies that the user agrees to disclose a list of personal data, the positioning of this explanation and the bundling of the actions of playing the game and giving consent may be misleading for data subjects. It is questionable whether clicking on the "Play Now" button is indeed a "clear, affirmative action" of the data subject. Moreover, satisfactory information about the purposes of data processing is not always available to the users. Therefore, the consent given in this case appears to be neither fully "informed" nor "specific".

Data subject-data subject interaction. In Facebook, even if a user does not consent to sharing some personal data, the actions of other users can reveal this data. Wall posts or comments by one user may contain personal data of others. A friend may make public a user's wall posts originally meant only for friends. Another relevant scenario is where user A wants to upload a photo including his friend user B on Facebook, but user B does not. It is also possible to infer personal data, not disclosed by the data subject, from that revealed by his network, i.e., his friends, friends-of-friends and groups [12]. Facebook privacy settings, which is a consent mechanism meant to enable users to control the personal data they share with their network, cannot deal with these scenarios.

'People You May Know" is an important Facebook feature that opens up the scope of data subject-data subject interaction by allowing one user to easily access the personal data of another. It suggests a user A's profile to another user B based on their mutual friends, common groups, networks (such as school, university, work) and uploaded contacts. In its current form, Facebook does not seek consent from A before suggesting him as a potential friend to B, increasing the accessibility of A's profile to B without A's consent. Like NewsFeed, this feature does not make more information publicly available, but makes it easier for a potential misuser to get to this

information [6].

4 Research Directions Towards Consent Compliance

While the lack of a consent mechanism deprives users of control over their personal data, a non-compliant consent mechanism can give users a false sense of control encouraging them to reveal more data than they would have otherwise. So, the research community must focus on converging towards GDPR compliant consent models that are acceptable to both users and service providers. To this end, we propose some research directions in this section. These research efforts would be multi-disciplinary in nature, involving the contributions of computer scientists, legal experts and psychologists.

Privacy Risk Evaluation for "Well-informed" Consent. A consent mechanism presents users with a set of choices. To help them make the right decision, the data controller should provide information about the data processing activity, its purpose and the personal data involved. However, there is a trade-off between in-depth, meaningful information and short, simple information that can be easily read and understood by an ordinary data subject. Users often do not read long privacy notices, yet they need deeper understanding and background to make informed choices. Even if they read, they lack the expertise to understand the consequences of their consents and are often ready to give up on privacy for small, immediate benefits [7]. In the Cambridge Analytica scandal, people gave up their own personal data and that of their friends in exchange for small monetary benefits. These data ended up being used to influence election results, a long-term harm for the society.

One way to address these problems in OSNs could be to design a tool that can assess on behalf of the user both long-term and immediate privacy risks of each consent. Usability surveys can help to construct the right interface for communicating these privacy risks to users. This risk information will be short, simple but concrete enough for the user to get a view of the consequences of their consent and help them arrive at a decision. In other words, it greatly enhances the "informed" characteristic of a valid consent. The GDPR, in its Recital 39, promotes this idea of making users aware of risks of personal data processing. Already, privacy risk evaluation has been utilized for other services to help users make meaningful choices of privacy settings [3].

Inter-provider and Intra-provider Risk Evaluation. Several pieces of data, aggregated over time, can lead to various privacy harms [7]. An average user may engage with several OSNs (not to mention other services) each of which usually involves several data processing activities. To truly avoid all privacy harms, the decision to consent for a data processing activity must depend on the consents already given to other data processing activities. Thus, researchers should focus on designing intra-provider and eventually inter-provider privacy risk evaluation mechanisms that take into account personal data revealed for all data processing activities for a given OSN and those for all OSNs that a data subject uses, respectively.

Balancing Privacy Risks and Social Benefits. Users have to deal with several cognitive and structural hurdles to arrive at meaningful decisions regarding consents to data processing activities [7]. Apart from privacy risks, they must also consider various social benefits, such as building new friendships and reviving and maintaining existing ones [2], for which they participate in OSNs. Automating the decision-making process of balancing privacy risks and social benefits for all data processing activities can take the burden off users. A similar approach was adopted recently to help users manage the privacy settings of OSN attributes [2].

Collaborative Consent and Risk-based Friend Selection. While the OSN provider is obligated to obtain valid consent to process data in the absence of another legitimate basis, other users are under no legal obligations to obtain the data subject's consent before sharing his personal data. Friends of a user may publicly share data that were meant to be seen only by friends or post photos of the user without the latter's consent. Potential misusers may also infer personal data of the user from the data revealed by his friends about themselves.

The design of collaborative consent mechanisms could be a fruitful research direction in this context. Using such mechanisms, a user and his friends can together decide which personal data they share and to what extent (i.e., keep it private, or share with friends, friends-of-friends or strangers) so that it is difficult to infer with high confidence any personal data that has been kept private. These mechanisms could also be used to resolve data disclosure scenarios where the user sharing some data is not the data subject (for example, a photo of A shared by B) or is only one of the data subjects (for example, a photo of A and B shared by B) [8]. Another solution approach could be to design mechanisms that enable users to choose friends based on the privacy risks they pose, both in terms of unintended disclosure and the inference of personal data from those revealed by the friends about themselves.

5 Conclusion

At present, consent mechanisms in OSN are either absent or are not compliant to the newly enforced GDPR. Such a scenario poses severe privacy problems for data subjects as the latter have no true control on their personal data. Consent compliance is an important step towards protecting user privacy. In this paper, we discussed the characteristics of valid consent according to the GDPR, analyzed the present status of consent in OSNs and proposed some research directions to arrive at GDPR compliant consent models that are acceptable to OSN users and OSN providers.

References

[1] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, 2018.

[2] S. J. De and A. Imine. To Reveal or Not to Reveal – Balancing User-Centric Social Benefit and Privacy in Online Social Networks. In *Proceedings of ACM SAC Conference*. ACM, 2018.

[3] S. J. De and D. L. Métayer. Privacy risk analysis to enable informed privacy settings. In *2018 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2018, London, United Kingdom, April 23-27, 2018*, pages 95–102, 2018.

[4] European Commission. General Data Protection Regulation, 2016.

[5] N. Fruchter, M. Specter, and B. Yuan. Facebook/Cambridge Analytica: Privacy lessons and a way forward. `https://internetpolicy.mit.edu/blog-2018-fb-cambridgeanalytica/`, 2018.

[6] G. Hull, H. R. Lipford, and C. Latulipe. Contextual Gaps: Privacy Issues on Facebook. *Ethics and information technology*, 13(4):289–302, 2011.

[7] D. J. Solove. Privacy self-management and the consent dilemma. *Harv. L. Rev.*, 126:1880, 2012.

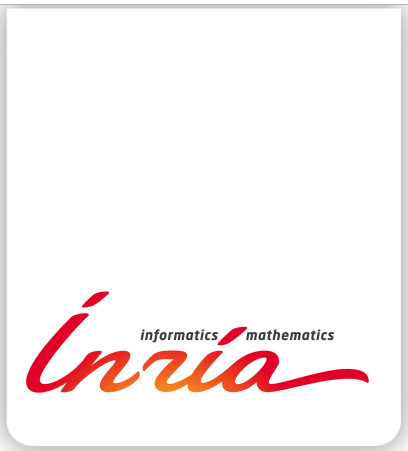
[8] A. C. Squicciarini, H. Xu, and X. Zhang. CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology*, 62(3):521–534, 2011.

[9] J. Sweeney. GDPR and the major social networks: what you need to know. `https://blog.makemereach.com/gdpr-facebook-twitter-snapchat-linkedin-what-you-need-to-know`, 2018.

[10] Times, New York. Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy. `https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html`, 2018.

[11] G. Venkatadri, A. Andreou, Y. Liu, A. Mislove, K. P. Gummadi, P. Loiseau, and O. Goga. Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface. In *IEEE Symposium on Security and Privacy (SP)*, pages 221–239, 2018.

[12] E. Zheleva and L. Getoor. To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles. In *Proceedings of the 18th international conference on World wide web*, pages 531–540. ACM, 2009.



RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399