ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# A Privacy Based Two Tales over Online Social Networks

**S.Laxmi Manasa**
M.Tech. Student,
Dept of CSE,
Indur Institute of Engineering and Technology,
Telangana, India.

**M.Komala**
Assistant Professor,
Dept of CSE,
Indur Institute of Engineering and Technology,
Telangana , India.

## ABSTRACT:

Privacy is one of the friction points that emerge when communications get mediated in Online Social Networks (OSNs). Different communities of computer science researchers have framed the 'OSN privacy problem' as one of surveillance, institutional or social privacy. In tackling these problems they have also treated them as if they were independent. We argue that the different privacy problems are entangled and that research on privacy in OSNs would benefit from a more holistic approach. In this article, we first provide an introduction to the surveillance and social privacy perspectives emphasizing the narratives that inform them, as well as their assumptions, goals and methods. We then juxtapose the differences between these two approaches in order to understand their complementarity and to identify potential integration challenges as well as research questions that so far have been left unanswered..

## Index Terms:

NOYB, Privacy, Cloud Computing.

## INTRODUCTION:

Can users have reasonable expectations of privacy in On-line Social Networks (OSNs)? Media reports, regulators and researchers have replied to this question affirmatively. Even in the "transparent" world created by the Facebooks, LinkedIns and Twitters of this world, users have legitimate privacy expectations that may be violated [9], [11].Researchers from different sub-disciplines in computer science have tackled some of the problems that arise in OSNs, and proposed a diverse range of "privacy solutions". These include software tools and design principles to address OSN privacy issues.Each of these solutions is developed with a specific type of user, use, and privacy problem in mind.

This has had some positive effects: we now have a broad spectrum of approaches to tackle the complex privacy problems of OSNs. At the same time, it has led to a fragmented landscape of solutions that address seemingly unrelated problems. As a result, the vastness and diversity of the field remains mostly inaccessible to outsiders, and at times even to researchers within computer science who are specialized in a specific privacy problem. Hence, one of the objectives of this paper is to put these approaches to privacy in OSNs into perspective. We distinguish three types of privacy problems that researchers in computer science tackle. The first approach addresses the "surveillance problem" that arises when the personal information and social interactions of OSN users are leveraged by governments and service providers.

The second approach addresses those problems that emerge through the necessary renegotiation of boundaries as social interactions get Password mediated by OSN services, in short called "social privacy". The third approach addresses problems related to users losing control and oversight over the collection and processing of their information in OSNs, also known as "institutional privacy" [17].Each of these approaches abstracts away some of the complexity of privacy in OSNs in order to focus on more solvable questions. However, researchers working from different perspectives differ not only in what they abstract, but also in their fundamental assumptions about what the privacy problem is. Thus, the surveillance, social privacy, and institutional privacy problems end up being treated as if they were independent phenomena.

Recent work in programming language techniques [4] demonstrate that it is possible to build online services that guarantee conformance with strict privacy policies. However, such approaches require buy-in from the service provider who, arguably, need the private data to generate revenue, and therefore have the incentive to do precisely the opposite.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The research question that we seek to explore therefore is to what extent a user can ensure his own privacy while benefiting from existing online services. The user unilaterally encrypting his data preserves privacy, however, doing so precludes search, and more importantly, breaks targeted ads. In order to preserve its bottomline, a cooperative service provider may re-engineer the service to provide privacy, or push ad targeting to the client. An adversarial service provider not willing to expend this effort, on the other hand, can simply deny service to unprofitable users.

To account for the latter case, a solution must protect privacy conscious users from being (easily) discovered. NOYB, short for none of your business, is based on the observation that some online services, notably social networking websites, can operate on "fake" data. If the operations performed on the fake data by the online service can be mapped back onto the real data, the user can, to a degree, make use of the service. Furthermore, privacy can be preserved by restricting the ability to recover the real data from the fake data to authorized users only.

This observation leads naturally to our solution: user data is first encrypted, and the ciphertext encoded to look like legitimate data. The online service can operate on the ciphered data, however, only authorized users can decode and decrypt the result. More broadly, NOYB proposes a new way of thinking about how to achieve privacy in online services whereby the user devises a transformation under which much of the functionality of the service is preserved, but which can only be undone by authorized users. The transformation is weaker than traditional encryption in that strictly more information is revealed to an adversary, but with the benefit that the victim can fly low under the adversary's radar by making it hard for the adversary to find the victim amongst ordinary users.

Such an approach can be deployed incrementally by small groups of users without buy-in from the service provider. Overall this paper makes three contributions. First, we present a general cipher and encoding scheme that preserves certain semantic and statistical properties such that online services can process the data oblivious to the encryption. Second, we show how to apply this general approach to Facebook.

And third, we report on our proof-of-concept implementation which demonstrates that NOYB is practical, feasible, and incrementally deployable by endusers without the need for additional infrastructure.Recent work in programming language techniques [4] demonstrate that it is possible to build online services that guarantee conformance with strict privacy policies. However, such approaches require buy-in from the service provider who, arguably, need the private data to generate revenue, and therefore have the incentive to do precisely the opposite. The research question that we seek to explore therefore is to what extent a user can ensure his own privacy while benefiting from existing online services.

The user unilaterally encrypting his data preserves privacy, however, doing so precludes search, and more importantly, breaks targeted ads. In order to preserve its bottomline, a cooperative service provider may re-engineer the service to provide privacy, or push ad targeting to the client. An adversarial service provider not willing to expend this effort, on the other hand, can simply deny service to unprofitable users. To account for the latter case, a solution must protect privacy conscious users from being (easily) discovered. NOYB, short for none of your business, is based on the observation that some online services, notably social networking websites, can operate on "fake" data.

If the operations performed on the fake data by the online service can be mapped back onto the real data, the user can, to a degree, make use of the service. Furthermore, privacy can be preserved by restricting the ability to recover the real data from the fake data to authorized users only. This observation leads naturally to our solution: user data is first encrypted, and the ciphertext encoded to look like legitimate data. The online service can operate on the ciphered data, however, only authorized users can decode and decrypt the result. More broadly, NOYB proposes a new way of thinking about how to achieve privacy in online services whereby the user devises a transformation under which much of the functionality of the service is preserved, but which can only be undone by authorized users. The transformation is weaker than traditional encryption in that strictly more information is revealed to an adversary, but with the benefit that the victim can fly low under the adversary's radar by making it hard for the adversary to find the victim amongst ordinary users.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Such an approach can be deployed incrementally by small groups of users without buy-in from the service provider. Overall this paper makes three contributions. First, we present a general cipher and encoding scheme that preserves certain semantic and statistical properties such that online services can process the data oblivious to the encryption. Second, we show how to apply this general approach to Facebook. And third, we report on our proof-of-concept implementation which demonstrates that NOYB is practical, feasible, and incrementally deployable by endusers without the need for additional infrastructure.

## EXISTING SYSTEM:

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by he recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

## Disadvantage:

- Opens up the possibility for hackers to commit fraud and launch spam and virus attacks.
- Increases the risk of people falling prey to online scams that seem genuine, resulting in data or identity theft.
- Potentially results in negative comments from employees about the company or potential legal consequences if employees use these sites to view objectionable.

## PROPOSED SYSTEM:

We distinguish three types of privacy problems that researchers in computer science tackle. The first approach addresses the "surveillance problem" that arises when the personal information and social interactions of OSN users are leveraged by governments and service providers. The second approach addresses those problems that emerge through the necessary renegotiation of boundaries as social interactions get mediated by OSN services, in short called "social privacy".

The third approach addresses problems related to users losing control and oversight over the collection and processing of their information in OSNs, also known as "institutional privacy".

## Advantage:

- The other major advantage is a subtle difference in policy between Facebook and OpenSocial.
- With Open Social, a third-party application can only query a user's friend data if both parties (user and friend) have consented and installed the application.

## PROBLEM STATEMENT:

We argue that these different privacy problems are entangled, and that OSN users may benefit from a better integration of the three approaches. For example, consider surveillance and social privacy issues. OSN providers have access to all the user generated content and the power to decide who may have access to which information. This may lead to social privacy problems, e.g., OSN providers may increase content visibility in unexpected ways by overriding existing privacy settings. Thus, a number of the privacy problems users experience with their "friends" may not be due to their own actions, but instead result from the strategic design changes implemented by the OSN provider. If we focus only on the privacy problems that arise from misguided decisions by users, we may end up deemphasizing the fact that there is a central entity with the power to determine the accessibility and use of information.

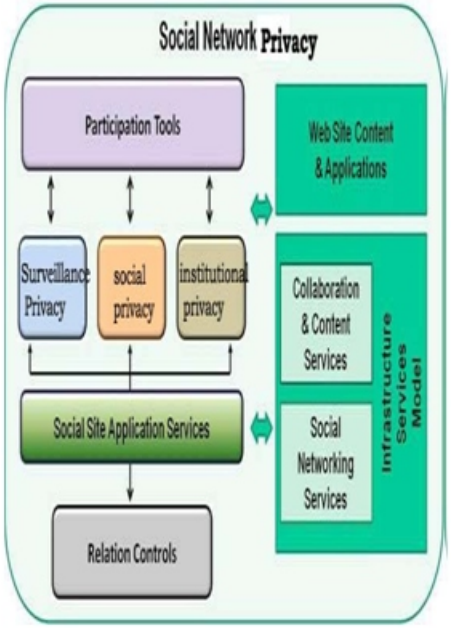
## SCOPE:

The first difference between the approaches lies in the way they treat explicit and implicit data disclosures. In the social privacy perspective, the privacy problems are associated with boundary negotiation and decision making. Both aspects are concerned with volitional actions, i.e., intended disclosures and interactions. Consequently, user studies are more likely to raise concerns with respect to explicitly shared data (e.g., posts, pictures) than with respect to implicitly generated data e.g., behavioral data). In contrast, PETs research is mainly concerned with guaranteeing concealment of information to unauthorized parties. Here, any data, explicit or implicit, that can be exploited to learn something about the users is of concern.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Shedding light on users' perception of implicit data may benefit both approaches. Studies showing how far users are aware of implicitly generated data may help better understand their privacy practices. The results of such studies may also provide indicators for how PETs can be more effectively deployed. If users are not aware of implicit data, it may be desirable to explore designs that make implicit data morevisible to users.

## ARCHITECTURE:




## MODULE DESCRIPTION:

Number of Modules After careful analysis the system has been identified to have the following modules:

1. The Social Privacy Module
2. Surveillance Module
3. Institutional Privacy Module
4. Approach To Privacy As Protection Module

### 1.The Social Privacy Module:

Social privacy relates to the concerns that users raise and to the harms that they experience when technologically mediated communications disrupt social boundaries. The users are thus "consumers" of these services. They spend time in these (semi-)public spaces in order to socialize with family and friends, get access to information and discussions, and to expand matters of the heart as well as those of belonging.

That these activities are made public to 'friends' or a greater audience is seen as a crucial component of OSNs. In Access Control, solutions that employ methods from user modeling aim to develop "meaningful" privacy settings that are intuitive to use, and that cater to users' information management needs.

### 2.Surveillance Module:

With respect to surveillance, the design of PETs starts from the premise that potentially adversarial entities operate or monitor OSNs. These have an interest in getting hold of as much user information as possible, including user-generated content (e.g., posts, pictures, private messages) as well as interaction and behavioral data (e.g., list of friends, pages browsed, 'likes'). Once an adversarial entity has acquired user information, it may use it in unforeseen ways – and possibly to the disadvantage of the individuals associated with the data.

### 3.Institutional Privacy Module:

The way in which personal control and institutional transparency requirements, as defined through legislation, are implemented has an impact on both surveillance and social privacy problems, and vice versa. institutional privacy studies ways of improving organizational data management practices for compliance, e.g., by developing mechanisms for information flow control and accountability in the back end. The challenges identified in this paper with integrating surveillance and social privacy are also likely to occur in relation to institutional privacy, given fundamental differences in assumptions and research methods.

### 4.Approach To Privacy As Protection Module:

The goal of PETs ("Privacy Enhancing Technologies") in the context of OSNs is to enable individuals to engage with others, share, access and publish information online, free from surveillance and interference. Ideally, only information that a user explicitly shares is available to her intended recipients, while the disclosure of any other information to any other parties is prevented. Furthermore, PETs aim to enhance the ability of a user to publish and access information on OSNs by providing her with means to circumvent censorship.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

## ATTACKING NOYB:

In this section we discuss attacks on NOYB components. While some aspects of security are ultimately rooted in components external to NOYB, such as the key management algorithm, the underlying cipher, and the steganographicscheme used, we consider only attacks on mechanisms described in this paper. The first line of defense for NOYB users is hiding in the crowd of ordinary users. Several NOYB mechanisms are geared towards this goal. First, cipher-text is encoded as legitimate atoms lacking any identifying tags. Second, the marginal distribution of the cipher-text atoms, and to some extent the joint distribution, matches that of legitimate atoms, which protects against Bayesian detection methods. Third, the partitioning into atoms preserves semantic relationships in the private information (e.g. name and sex are kept together) to make it harder to develop heuristics to semantically detect encrypted information. Fourth, steganography is using sparingly to minimize the chances of detection. Fifth, the public dictionary is padded with information of non NOYB users to increase the rate of false positives if an adversary were to pick users matching dictionary atoms at random. And sixth, communication across different channels is decorrelated to avoid timing attacks. That said, in the event the online service does discover a NOYB user, the service does not learn the private information, and can at best deny the user service if the terms of service so allow.

## USING NOYB IN FACEBOOK:

We now delve into the finer details of applying NOYB to Facebook. As mentioned previously, our goal is to preserve user privacy while allowing users to make use of Facebook to advertise themselves to their extended social network. Facebook profiles contain over 40 fields of personal information; we mention some illustrative examples of how these are partitioned into atoms that are small enough to not leak much information, and yet large enough to be internally consistent. For instance, the name and sex of a person are contained within a single atom for consistency.Similarly, the street address, city, state, country and the area codes of telephone numbers are contained within another atom. For fields that contain lists, such as personal interests, favorite music, movies and tv shows, each list element is a separate atom.

Other fields such as birthdate, political and religion views, etc. each represent a separate atom. However, not all fields are partitioned into atoms. The key omissions are the phone number (excluding the area code), the user part of email addresses, and instant messaging handles. This is because these elements are expected to be unique; the substitution process cannot guarantee that cipher-atoms will also be unique, and indeed due to the birthday paradox, it is likely that even a small userbase will generate some duplicates that may be noticed. Fortunately, there is little internal structure to these fields, which allows the substitution to be applied at the character level, with the dictionary comprising the alphabet (with character frequencies) [15].

## IMPLEMENTATION:

We implemented a proof-of-concept version of NOYB as a browser plugin for the Firefox web browser. Our implementation modifies Facebook pages by adding a button that encrypts the user's own profile. A second button added to other user's pages decrypts their profile. The plugin consists of 1400 lines of XUL code, and 500 lines of python code that uses AES in counter mode as the underlying cipher. The dictionaries necessary for the plugin are generated by a service we built; the service samples Facebook profile pages of NOYB users and non-users, and posts the dictionary to a public website that NOYB users can query anonymously.

At present, our implementation does not manage keys and instead defers to the user at the time of encryption and decryption to enter the password, however, it is possible to modify our plugin to automatically distribute keys to the friends, and receive keys from friends through web based email services. We have manually verified that the encrypted profiles look plausible without revealing significant private information. We are quick to point out, however, that our experience is limited owing to our small userbase. A second purpose of our implementation exercise is to study the feasibility of maintaining the dictionaries. We find that the size grows sublinearly reflecting overlapping values across different users. While the numbers are encouraging in that we expect a dictionary of a million users to initially be manageably small (344 MB), we do not, at present, have data to comment on the size of the dictionary over time as new atoms are appended.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Nevertheless we believe that if the size grows by up to 3–4 orders of magnitude over the lifetime of the online service, a distributed peer-to-peer dictionary infrastructure could be necessary.

## RELATED WORK:

User privacy has been an active field of research stretching back to the beginnings of public and commercial adoption of the Internet. Pretty Good Privacy (PGP) [20] applies endto-end public-key cryptography to emails. TLS [7] applies the same to end-to-end interactive communication channels. While NOYB is similarly end-to-end in the privacy it provides, it is different from the aforementioned systems in that it is not completely opaque to the middle, and can therefore make greater use of the functionality provided by the online service. A second class of privacy preserving services operate in the middle of the network. Such services include anonymizing proxies [8], and dark nets [5]. These services provide an all-or-nothing model to privacy, where the privacy preserving mechanism, such as stripping of a HTTP cookie, either completely shields the user potentially breaking the application, or, when absent, leaves the user completely vulnerable. NOYB, instead, is tightly coupled with the application allowing fine-grained control over user privacy while balancing the functionality preserved. Complementary to NOYB is the large amount of research in ciphers, key management, steganography, and DHTs. NOYB shares a resemblance to the pseudorandom character substitution cipher in [15]. Particularly of use to NOYB are existing and future broadcast key management algorithms [3], strong underlying ciphers [6], resillientsteganographic techniques [11], and distributed store-lookup infrastructures [14], which can be used to implement the external mechanisms that NOYB relies on.

## CONCLUSION AND FUTURE WORK:

By juxtaposing their differences, we were able to identify how the surveillance and social privacy researchers ask complementary questions. We also made some first attempts at identifying questions we may want to ask in a world where the entanglement of the two privacy problems is the point of departure. We leave as a topic of future research a more thorough comparative analysis of all three approaches. We believe that such reflection may help us better address the privacy problems we experience as OSN users, regardless of whether we do so as activists or consumers.

## REFERENCES:

[1] Alessandro Acquisti and Jens Grossklags.Privacy and rationality in individual decision making. IEEE Security and Privacy, 3(1):26 – 33, January/February 2005.
[2] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano.Privacy-Enabling Social Networking over Untrusted Networks. In ACM Workshop on Online Social Networks (WOSN), pages 1–6. ACM, 2009.
[3] Miriam Aouragh and Anne Alexander. The Egyptian Experience: Sense and Nonsense of the Internet Revolutions. International Journal of Communications, 5:1344 – 1358, 2011.
[4] F. Beato, M. Kohlweiss, and K. Wouters. Scramble! your social network data. In Privacy Enhancing Technologies Symposium, PETS 2011, volume 6794 of LNCS, pages 211–225. Springer, 2011.
[5] B. Berendt, O. Gunther, and S. Spiekermann. Privacy in E-Commerce:¨ Stated Preferences vs. Actual Behavior. Communications of the ACM, 48(4):101–106, 2005.
[6] E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams.Humming bird: Privacy at the time of twitter. In IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.
[7] A. Cutillo, R. Molva, and T. Strufe.Safebook: A privacy-preserving online social network leveraging on real-life trust. Communications Magazine, 47(12):94–101, 2009.
[8] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second generation onion router. In USENIX Security Symposium, pages 303,320, 2004.
[9] FTC. Ftc charges deceptive privacy practices in google's rollout of its buzz social network. Online, 03 2011.
[10] Glenn Greenwald. Hillary clinton and internet freedom. Salon (Online), 9. December 2011.
[11] James Grimmelmann. Saving facebook. Iowa Law Review, 94:1137,1206, 2009.
[12] Kevin D. Haggerty and Richard V. Ericson. The Surveillant Assemblage. British Journal of Sociology, 51(4):605 – 622, 2000.
[13] Heather Richter Lipford, Jason Watson, Michael Whitney, Katherine Froiland, and Robert W. Reeder. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In Proceedings of the 28th international conference on Human factors in computing systems, CHI '10, pages 1111–1114, New York, NY, USA, 2010. ACM.