Modularity is the Key: A New Approach to Social Media Privacy Policies

Jayati Dev
Indiana University
Bloomington
jdev@iu.edu

Sanchari Das
Indiana University
Bloomington
sancdas@iu.edu

Kaushik Srinivasan
Indiana University
Bloomington
kausrini@gmail.com

1. INTRODUCTION

Social media privacy policies are legal statements which provide details about the collection, storage, and access to user data which are often long and convoluted for an average internet user to read [1, 3]. Rich literature exists on improving the accessibility of these privacy policies but only faintly hints at the need for the flexibility in user choice. Our goal in this study is to (i) develop a conceptual model for highlighting privacy policy statements to improve clarity and visibility in the policy-making and (ii) to conduct user studies to see if better policy design improves privacy decision-making. This study examines the loopholes in existing social media privacy policies especially that of Facebook and targets to map the policy statements to the distinct services offered, allowing users to agree to specific services which they wish to use, essentially making the overall policy non-binary in nature. Additionally, it also would encourage developers to easily integrate privacy policies when new features are added to a service platform.

2. METHODOLOGY

In order to enhance the effectiveness of data policies and reduce its complexity for the readers to comprehend in a better way, we propose a Modular Privacy Policy Model (MPPM). We divide data access policies into separate modules according to the respective services offered by Facebook. This enables the users to clearly see what kind of data is collected by each of the services and allows them to only agree or disagree to specific sections of a privacy policy. However, we also acknowledge that in an attempt to condense a verbose privacy policy which factors in legal terminology, it is likely that certain subtleties might be lost. The target of the prototype was easy readability and this can be extended to provide legal documents to the users. We draw from two design principles proposed by Dan Norman [4] - (i) developing a conceptual framework for better comprehension and (ii) improving clarity and visibility in the policy model.

MPPM attempts to provide user assurance that certain data would not be collected by social media platforms, specifically Facebook. The different sections that we have formed in the modular policy can be broadly classified into the following categories – (i)services offered, (ii) data collected (including permissions like microphone, camera, etc.), (iii) how the data is being used, (iv) default consent settings, (v) location and duration of data storage. For each of the services that Facebook provides, we define policies in these categories mentioned for data collection, usage, and storage. The specific Facebook services that we have considered in our model are 'Find Friends', posting (texts, photos and videos), Facebook Messenger, pages, events and check-ins, games & third-party services and Facebook payments. Generic user modeling systems [2] provide a basic framework for studying how users value their privacy.

We create MPPM this by implementing the following design iterations – *i) Study the current data policy by Facebook, ii) Develop sections for classification derived from the data policy, iii) Extract sections from policy and fit into the classification of service to policy mapping, iv) Develop the modular sections of the policy based on the extracted data, and v) Validate the usability of the modular policy by conducting qualitative user studies.* At the user end, these service-specific policy statements can be seen and accepted in parts according to the particular service they desire.

3. DISCUSSION

The MPPM proposed in this paper provides the user with options to take control of their privacy by selectively agreeing to only sections of the privacy policy corresponding to specific services offered by the platform which a user might or might not choose to use. Through our modularized design we attempt to increase transparency between an organization and its users, which will not only enhance the user experience, but also increase the trust of a user on a company with their data. Additionally, policy makers will find it more convenient to implement sections in the privacy policy when they develop or upgrade new services without modifying the entire privacy statement. Finally, we also would like to make our concept generalizable to privacy policies across organizations in future work and conduct usability studies to understand the effectiveness of our design through user participation.

4. REFERENCES

[1] M. Fishbein and I. Ajzen. Belief, attitude, intention, and behavior: An introduction to theory and research. 1977.

[2] A. Kobsa. Generic user modeling systems. *User modeling and user-adapted interaction*, 11(1):49–63, 2001.

[3] A. M. McDonald and L. F. Cranor. The cost of reading privacy policies. *ISJLP*, 4:543, 2008.

[4] D. Norman. *The design of everyday things: Revised and expanded edition.* Basic Books (AZ), 2013.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.