Social Networking Privacy: Understanding the Disconnect from Policy to Controls

Pauline Anthonysamy, Phil Greenwood, Awais Rashid
School of Computing and Communications, Lancaster University, Infolab21, Lancaster LA1 4WA, United Kingdom.
E-mail: {anthonys, greenwop, marash}@comp.lancs.ac.uk

Abstract

Social networking sites have become increasingly popular over recent years. However, there is a widespread level of dissatisfaction and lack of trust from users towards social network providers due to privacy concerns. This article attempts to uncover whether these feelings are justified by examining the degree of traceability between privacy policies and the privacy controls of social networking sites. Our aim was to determine whether the privacy controls actually reflect the contents of the privacy policies. We studied sixteen prominent social networking sites and discovered that there is a significant disconnect between privacy policies and privacy controls.

Keywords: Social Networks; Traceability; Privacy; Policy; Controls;

I. INTRODUCTION

Social networking sites (SNS) are leading a new era of communication and a pathway to a world without boundaries. According to [1], in 2008 more than 30% of Internet users were members of at least one SNS – with recent statistics showing that Facebook alone now has more than 900 million users. Although SNS have many benefits, these are often negated by privacy concerns. For example, until recently fixed, Facebook applications were leaking access tokens that enabled the collection of private user profile information. Similarly, Myspace had a fault which permitted public access of private photos despite assurances to the contrary in their privacy policy.

As a result of such lapses, there is an increasing level of dissatisfaction and lack of trust from the users of such SNS towards the social network providers. Users are pushing for more clearly defined privacy policies and privacy controls so that they can be aware of how their data is managed. Similarly, governments are issuing directives such as the EU’s Data Protection Directive [3], and the US Federal Trade Commission [4], which require SNS to provide privacy policies to ensure social network providers take responsibility for the privacy of their members’ personal information. SNS themselves are taking steps to address the privacy concerns of users and other organisations by continually tweaking and updating their privacy policies and controls. Despite all of these efforts, there is evidence that SNS users

1 www.dailyherald.com/article/20120428/business/704289974/
2 www.symantec.com/connect/blogs/facebook-applications-accidentally-leaking-access-third-parties
3 www.wired.com/politics/security/news/2008/01/myspace
still generally know little about how their personal information is managed [5] and find privacy controls inherently difficult to understand and configure [6].

One way of enhancing user trust is for social network providers to demonstrate that they have taken effective measures to protect users’ personal information. A critical step towards achieving this is to confirm that the actual functionality provided by the SNS, via privacy controls, is consistent and reflective of its privacy policy. Given this, the question that naturally emerges is whether it is possible to establish a traceable mapping between the policy and controls so that, by reading the former and using the latter, a user can establish a direct relationship between them? This article explores this very question by comparing the externally observable relationships between the content of privacy policies and the functionality of privacy controls of sixteen prominent SNS. The externally observable relationship indicates a user’s perspective of interacting with a social network – from this perspective, the user’s available interactions are realised through the privacy controls of the SNS and their relationship with the SNS’ privacy policy.

Existing work for examining such concerns focuses either on ensuring software requirements compliance with governing legal texts and privacy policies [7], [8] or on measuring the correctness and usability of privacy controls in SNS [9], [6].

Efforts surrounding compliance have centred upon extracting requirements directly from privacy policies [8], [10] or from legal documents [7]. In contrast, the question that we explore is whether the runtime functionality provided by privacy controls is a true reflection – that can be traced back – of the statements in the privacy policies in the highly volatile domain of SNS. The results of this analysis can provide insights into whether existing compliance checking mechanisms employed by SNS are indeed effective. Establishing a clear traceability relationship will benefit both users (providing clearer guidance on how their information is handled) and SNS (validating the compliance exercise and increasing users’ trust).

From the perspective of correctness and usability, Bonneau et al. [9] conducted a comprehensive privacy study across 45 SNS from an economic angle, which looked at the diversity of data collected by the sites, the types of privacy controls, promotional methods etc. Other studies [6], [2] have examined social network users’ and the general public’s perception of privacy on SNS. All of these studies found that, generally, people’s knowledge of how social media functions in regards to use, disclosure and transfer of their personal information is largely inadequate and users have difficulty configuring their privacy settings.

In previous work [11], we performed an exploratory study of four SNS that examined their privacy policies in terms of three high-level categories and highlighted the general disconnect between privacy policies and privacy controls. This article builds on those initial insights and provides a detailed analysis of the externally observable relationships between privacy policies and controls of 16 SNS by applying a systematic traceability methodology. This methodology is based on a taxonomy of SNS privacy policies and a detailed mapping...
between the privacy policy statements and privacy controls. Our analysis answers the following questions:

1) What are the common themes of information addressed in the privacy policies of SNS?
2) What are the privacy controls that are available to users of SNS?
3) Do traceable relationships exist between the information addressed in a site’s privacy policy and the site’s corresponding privacy controls?

For the purposes of this study, we perceive privacy policies as a set of **actions** performed by SNS on information supplied by a user and privacy controls as **operations** that are presented to users to manage their personal information. Our findings indicate a significant disconnect between policy statements (actions) and privacy controls (operations). Two-thirds of the privacy categories were evaluated as **partial or broken** in terms of their traceability.

**II. DATA SOURCES**

In order to determine the levels of traceability between privacy policies and privacy controls, we analysed the privacy policies and privacy controls of 16 prominent SNS. The data collection and analysis were performed between January & May 2011.

We selected 16 popular SNS (the list can be found in Fig. 2) as our data sources. The sites chosen provide typically functionalities, such as conversing with other members, creating profiles, sharing photos and videos, etc. Furthermore, these sites met a number of criteria necessary for our analysis: i) the sites had a large number of active global users; ii) their privacy policies were available online; iii) the sites provided a variety of privacy controls to their users.

The first step of our data collection involved taking a snapshot of each site’s privacy policy as it would be presented to a non-member. Next, we created four test accounts on each site: two for **adults** (18 years and above) and two for **minors** (between 13 and 17 years). These four accounts allowed us to examine the visibility of one profile from another and to identify any differences between adult and minor accounts. Each of these accounts were made “friends” (or equivalent) with each other.

When creating these accounts, we recorded all information requested and provided the same profile information (e.g. name, birth date, email, etc.) for each site. Optional information was also included to make comparisons across sites and to determine the default visibility of this information. Next, observations were made regarding the profile information that was publicly viewable (via SNS search features, public URLs of the profiles, and external search engines) and the profile information visible from “friend” accounts via these same sources. Finally, a record was made of all the privacy controls that were available to users and their

---

6 There exists a distinct set of regulatory codes that governs the access of minors on SNS.
7 Complete profile information can be found at [http://www.comp.lancs.ac.uk/~anthonys/dataset.html](http://www.comp.lancs.ac.uk/~anthonys/dataset.html)
8 Observations were made when logged into an adult “friend” account and viewing a minor’s profile and vice-versa.
default values. These default settings were maintained throughout this data collection process.

Our data collection and analysis procedures were carried out by one person and then independently reviewed and verified by a second person. Any conflicts that arose while checking the data were resolved by referring back to the details of our traceability method [12] to establish the correct course.

III. MODELLING AND EVALUATING TRACEABILITY RELATIONSHIPS

Determining the degree of traceability between SNS’ privacy policies and privacy controls is complex due to the granularity difference between the two. We overcame this complexity by identifying a set of common reference points between statements of the privacy policy and the privacy controls of the SNS that allowed us to establish a mapping. Subsequently, we determined the degree of the traceability by applying a scale to the mappings identified.

A. Mapping Procedure

Our common reference points over which to perform privacy policy ↔ privacy control mapping are data and visibility. This represents the fundamental model of SNS in which users submit data and can choose (or are required) to make that data visible to others. We then model the statements of a privacy policy as a set of actions over data and visibility, and privacy controls as a set of operations over data and visibility. Our mapping procedure involves, where possible, the establishment of clear mappings from each action-statement of a privacy policy to a corresponding operation of a privacy control.

To aid in analysis of privacy policies in particular we used content analysis [13] to categorise segments of qualitative data into meaningful themes. We decomposed privacy policy statements and examined the contents of each statement to identify the ‘actions’ performed by a SNS in terms of data and visibility. Actions, expressed by verbs or verb phrases in natural language, depict the manipulations that are performed with regards to the data provided by a SNS user. We applied this process to each SNS to identify a refined set of common categories/themes (see Fig.2 for full list). Further inspiration for categorisation was drawn from Anton et al.’s work [14].

Finally, where possible we cross-referenced (mapped) the decomposed statements with privacy controls (‘operations’). Our mapping procedure applies the following three steps to each category identified above:

1) For each statement in each category attempt to identify a corresponding operation that maps to the action of the statement by matching terminology (terms that have the same meaning in describing the actions and operations) across the two.
2) Verify that the data item(s) manipulated by the control operation match those mentioned in the statement.
3) Verify that the default visibility of this data, as indicated by the operation, is consistent with that specified in the policy statement.
Consider the example in Fig. 1. Facebook’s privacy policy has statements relating to social adverts. By matching the terminology used, we mapped this statement to the corresponding ‘Advertising’ operations. Here, the term ‘social ads’ from the privacy policy statement maps to the operation described as ‘Edit social adverts setting’, i.e. the term ‘social adverts’ has the same semantic definition as ‘social ads’.

Next, we verify the data items managed by the identified privacy controls match those mentioned in the privacy policy statement. Occasionally, this verification can be non-trivial due to ambiguous or imprecise terms being used. In such cases we extrapolated the data items based on examples provided by the SNS when describing this operation (see Fig. 1) or checked whether generic catch-all terms (e.g. “personally identifiable information”) are defined elsewhere by the SNS. Finally, we verify the default visibility value of the matched operation as shown in Fig. 1 to that specified in the policy statement i.e. friend.

**B. Mapping Scale**

To qualitatively evaluate the mappings between privacy policies (actions) and privacy controls (operations) we needed to develop a new kind of mapping scale to fit the unique requirements of our analysis. This scale assesses the degree to which each operation fulfils the actions described and consists of three ratings: complete, partial, and broken.

**Complete:** To be considered complete, the mapping between the privacy policies and controls should meet two fundamental properties: (1) *Consistent:* - refers to lack of
contradiction between statements in privacy policies and controls. This is evaluated based on consistent use of terminology, where terms and words with the same semantic meaning are used to describe actions and operations. The data items should also be identical and match the default visibility. (2) Unambiguous: the information can only be interpreted in one way (i.e. explicit specification of actions) and the actions easily related to one or more operations of a SNS.

For example, this text from Twitter’s privacy policy “Information Collected Upon Registration: When you create ... account, you provide some personal information, such as your name, username, password and email address. Some of this information, for example, your name and username, is listed publicly ...” was considered complete when mapped to its operations as this precise set of data items was collected during sign-up and the specified visibility applied.

**Partial:** A partial mapping is defined by two properties: (1) Imprecise: refers to missing/unspecified and indirect information. Indirect information is information that is specified subtly, i.e. which is there for the purposes of compliance with regulations but not intended to be noticed by a user (e.g. opt-in/out links buried within the policy text). (2) Ambiguous: terms or phrases in policy statements that are vague or can be interpreted in multiple ways (e.g., generic terms like “personal information”).

For instance, PerfSpot’s privacy policy states: “We use 3rd party advertising companies to serve ads... These companies may use information (not including your name, address, email address or telephone number) about your visits... If you would like more information about this practice and to know your choices about not having this information used by these companies, click here”. Although a URL is provided from the privacy policy, where the user can opt-in/out of advertisements, there were no specific operations within the sites’ privacy controls that could be matched to these statements and so was assigned as an imprecise mapping. Furthermore, the data specified was imprecise as it defines the data to be excluded and not the data that will be included.

**Broken:** Mappings are marked as broken if they meet one property: Disjoint: which refers to instances where statements (actions) specified in a privacy policy could not be matched to any operations. This implies that a traceability relationship does not exist since the actions are not operationalised into privacy controls. For instance, most of the SNS state they collect certain data indirectly i.e. non-identifiable information, IP address, operating system, page views. However, there are no specific operations that let a user decide if s/he wishes to share these data. This may result in users providing information in an involuntary manner.

**IV. FINDINGS**

Our analyses enabled us to assess the degree of traceability between privacy policies written in natural language text (categorised as actions) and the existing privacy controls (operations) of SNS. The final results are summarised in Fig. 2. The column on left of Fig. 2 illustrates our complete refined set of action categories according to the common characteristics that emerged when examining the various privacy policies of the 16 sites. High-order categories
give an overview of the actions described in a privacy policy, while lower-order categories allow for finer distinctions to be made within and among specific categories of actions.

<table>
<thead>
<tr>
<th>Privacy Policy Categories</th>
<th>Facebook</th>
<th>MySpace</th>
<th>LiveJournal</th>
<th>tube</th>
<th>Badoo</th>
<th>MyFave</th>
<th>Hi5</th>
<th>Tagged</th>
<th>Netlog</th>
<th>tubeco</th>
<th>myplace</th>
<th>Friendster</th>
<th>Orkut</th>
<th>LiveSpace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PI / Registration information</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Indirect collection</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Information gathered passively</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Communication</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Advertising</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Aggregation</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Personalization</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Information Sharing</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Sharing by a member</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>With other users</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>With 3rd parties</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Sharing by the SNS provider</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>With 3rd parties</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>With law enforcement</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Information Management</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Review/change personal information</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Information removal</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Information Monitoring</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>By SNS provider</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>By 3rd parties</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Information Protection (for specific groups)</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️ ✔️</td>
</tr>
</tbody>
</table>

Legend: ✔ Complete ▼ Partial - Not Applicable

Fig. 2. Degree of Traceability from the Mapping Process. Cells are marked as indicated in the legend. Each marking in the cell represents the result of the individual mapping of each of the privacy policies’ statements in that category and the corresponding privacy controls.

The table cells are marked as shown in the legend indicating the degree of traceability. Cells are marked with “-” where mapping was inapplicable or when the site did not specify the information required for evaluation. Each cell represents the individual mapping of each of the privacy policies’ statements (actions) in that category and the corresponding privacy controls (operations). A category of a privacy policy that contains 3 statements, for example, has three markings in the corresponding cells of our table.

Our overall findings indicate a significant disconnect between policy statements (actions) and privacy controls (operations) – two-thirds of the evaluated categories. We examine the results for each policy category in detail (based on the specific statements within a category). Note that the discussion is not exhaustive but rather highlights selected interesting observations.

A. Complete Traceability

The following category was evaluated as having generally complete traceability across the studied sites.

- The studied sites all have a clear and transparent age requirement for users in their privacy policies in accordance with the US Federal Trade Commission [4] (or
[3] for the EU). For example, consider this statement from Tagged’s privacy policy: “Tagged is a general audience web site that complies with the Children’s Online Privacy Protection Act (COPPA). Our registration process is designed to restrict children under the age of 13 from becoming members of Tagged and using our site.” This statement was classified within the ‘Age Restriction’ sub-category, based on the verb restrict (action). We then identified the data item involved as age. We were then able to map this statement to an operation on Tagged during sign-up, where registration fails when we tried to sign-up using a birth date that violated the site’s age requirement. This statement was therefore evaluated as a complete mapping. We were able to establish such complete mappings on 12 sites that had statements describing age restrictions for sign-up in their privacy policies. Note that although we marked the mappings as complete for these sites, our observations show that the age restrictions imposed by the sites can be easily bypassed during sign-up. We attempted this for a few sites and found that 3 of 12 sites allowed one to sign up by just changing the birth date (making it adhere to the sites’ age requirement) while the remaining 9 sites needed the browser cookies to be cleared in order to proceed. 4 sites did not state any such restrictions on their privacy policies but we found that restrictions were imposed during sign-up (marked as ‘-‘ in Fig. 2).

B. Partial Traceability

The following categories were evaluated as having generally partial traceability across the studied sites.

- **SNS can be vague regarding data that is collected.** Precise definition of data categories is vital to understand the significance of some information compared to others. This is particularly important when determining which piece of data may enable a person to be identified if shared with 3rd parties. A vast majority of the privacy policies examined have imprecise and ambiguous descriptions of the different data types that are collected. Consider this statement from Orkut’s privacy policy which describes its data collection practices: “As an Orkut member, you can create profile or Orkut community that includes personal information, such as your gender, age, occupation, hobbies and interests plus other content, such as photos.” According to our observation only a small number of data items specified in their privacy policy could be directly mapped (traceable) to ones that were actually collected\(^9\). This is because they tend to over-use catch-all terms such as “other content” without defining what such terms constitute. We therefore evaluated this statement as ‘partial’ for the ‘Optional Information’ category. Our results show that only 6 sites had precise definitions, and therefore ‘complete’ mappings (for all statements), on the ‘Registration Information’ that they collected, while only 4 had complete mappings for the optional information.

---

\(^9\) Complete data collection can be found at http://www.comp.lancs.ac.uk/~ anthony/s/dataset.html
• **SNS fail to communicate default visibility settings.** Most of the surveyed sites use role-based access control mechanisms\(^\text{10}\) to manage one’s personal information. 14 sites included statements explaining the type of information one can share and with whom in their privacy policy. We were able to map these statements to the corresponding operations found on these sites (as illustrated in Fig. 2). However, we found that 10 of the 14 sites failed to communicate the default configurations (which are mostly ‘Public’) that come with a new profile. Only two, Orkut and Live Space, made ‘Friend’ grouping as the default configuration.

We also found that 10 of the 16 sites implemented a restricted sharing mechanism for minor users. Facebook, Orkut, Tagged, MySpace (to name a few) made the visibility of profiles of users under 18 private/restricted by default. MySpace and Facebook had an operation that disallowed minor profiles from being searchable by default. Although the sites provided a distinct set of privacy configuration for minors, we found that the default settings were switched automatically to the configuration of an adult’s account (more public) when the user turns 18. The users are not made aware of the change when it happens.

*C. Broken Traceability*

The following categories were evaluated as having generally broken traceability across the studied sites.

• **Users have no control over indirect data collection.** Nexopia states in its privacy policy that “Nexopia.com also logs non-personally identifiable information of members and visitors to the site, including IP address, aggregate user data, and browser type. This information may be shared with 3rd parties ....” However, no operations were found on this site that enabled one to opt-in/out of this collection activity and neither were the specific data items which are subject to collection defined i.e. the specified list is illustrative but not exhaustive. Similar observations were made on 15 sites where the mappings for this action were consistently evaluated as broken across these sites except for Orkut. Orkut is governed by two privacy policies - one from the social network itself and a second one from Google. Orkut’s privacy policy excluded information on indirect data collections. However, this was covered under Google’s privacy policy. Our study is primarily focused on the privacy policies of the SNS itself which makes Google’s privacy policy out of the scope of our study. We therefore marked the corresponding mapping as inapplicable.

• **Users cannot opt-in/out of any SNS internal processing activities.** As an example, consider the following statement from Badoo’s privacy policy: “We internally use personal information of our users to statistically analyse site usage, to comply with applicable law, to improve our content and product offerings ...” It is clear that this fails to explicitly specify the data items that will be used and to whom they might be accessible. Additionally, we were unable to identify and match any operations with

\(^{10}\) A mechanism that provides the ability to segregate people into abstract, self-defined groups and make access control decisions at the group level.
this usage activity and we therefore marked this mapping as broken. All sites had similar statements in their privacy policies for the ‘Internal Usage’ category but none of them had an equivalent operationalised control. This was also the case for the statements classified under the ‘Aggregation’ category in which 12 sites state that they aggregate users’ information, but none of them allow the user to control this action.

- **SNS give users no control to prevent data being shared with advertisers.** Our results indicate that users are not given any form of control in restricting SNS providers from sharing their information with third-parties. As an example, Bebo states in its privacy policy that “Bebo may transfer information about you and your use of Bebo, such as your IP address, information stored via cookies, and other demographic information about you, to our advertising affiliates (such as Advertising.com), partners (including Yahoo! and its affiliates) and other third parties”. The documented visibility of the identified data items (marked in bold) was advertising affiliates, partners and other third parties. Once again, catch-all terms were used in describing the data that will be shared and with whom, i.e. illustrative but not exhaustive, and we found no corresponding operations to restrict this action. We therefore marked this mapping as broken. In total 15 sites indicated that user data will be shared with 3rd parties with no corresponding operations to control this sharing.

### D. Multifarious Traceability

Finally, the following categories were evaluated as having a varied degree of traceability across the surveyed sites.

- **Users are given little support to discover and understand 3rd party privacy policies.** Most of the SNS state that data may be shared with 3rd parties if: one adds an application, follows links to other sites or clicks on adverts, but do not provide traceable details on the specific data items that are shared and with which 3rd parties. As an example, consider Orkut’s privacy policy which specifies that “You may choose to use an application by adding it to your profile. If you add an application to your profile, the application may collect information from your profile or other information about your activities on Orkut and share that information with others”. Firstly, this statement uses catch-all terms (not defined in Orkut’s privacy policy) to describe the data items that are shared and their visibility, also we were unable to identify any operations that allowed us to control this sharing. We therefore marked this mapping as broken.

Conversely, Facebook and LinkedIn explicitly specified the data that might become visible when one adds an application. Accordingly, we found operations that allowed us to control (some of) the data that will be shared. We also observed that a few of the remaining sites post a link to the third-party’s privacy policy when one tries to connect to an application on the site. Users are left to their own discretion for finding these privacy policies, discovering which terms apply to their use of the application in the specific SNS and how these may impact on their privacy. In total 10 sites had
statements indicating that data may be shared with 3rd parties directly of which 5 had broken mappings.

- **Removing personal information is difficult.** 12 sites addressed account removal in their privacy policies but it was inconsistently mapped to the privacy controls. As an example, Hi5’s privacy policy states that: “If you would like to **delete your account**, log into hi5, go to your account settings page by clicking the account link in the top right hand corner. On that page, right below the email address field you will see a link to **cancel your account**”. Although we found the matching operation on the settings page, the operation did not delete the account but instead just deactivated the account. Similarly, Facebook’s privacy policy specified that users can either deactivate their account or remove it permanently. However, when identifying the corresponding operations we were able to find only a deactivation link on the settings page while the deletion link was only accessible through their privacy policy (indirect mapping).

We also found that Myspace, Hyves and Friendster did not include any information on data removal in their privacy policies. However, we found deletion and cancellation operations on these sites. For instance, in its settings page Hyves indicated that removal of one’s account will permanently delete all profile information. Although we were able to verify that the accounts were in fact removed the process of locating this operation was complicated and unclear (buried among other settings). Hyves’ omission of explicit instructions on account removal places the burden on users to discover how one can delete his/her account. Perhaps of greater concern is Perfspot’s omission of information on data removal. Its privacy policy neither included information on account deletion nor provided any operations to do so.

- **Passive data collection is poorly defined.** Automated observation of user behaviour reveals the applications one uses, web pages visited, music listened to, and so on. As an example, consider these two statements from Perfspot’s privacy policy: (1) “PerfSpot may use session cookies and persistent cookies for the purpose of tracking various important data ... While we recommend that you allow these cookies ..., you may adjust your computer’s settings to restrict or refuse them.” (2) “PerfSpot uses clear .GIFs and log file data to ... monitor the impact..... marketing efforts ... monitor aggregate metrics providing detailed data on User activities while on the Website”. In accordance to statement 1, we were able to block the cookies by configuring the browser settings (operation) however, this can be a non-trivial task especially for a non-technical user (indirect mapping) and therefore evaluated this statement to be ‘partial’. As for statement 2, we were unable to identify any corresponding operations relating to this action on Perfspot hence evaluated it to be ‘broken’.

The privacy policies of the surveyed sites also include statements that indicate monitoring technology can be placed by 3rd parties. We found that 6 sites provided a link to Network Advertising Initiatives Opt-Out program where users can opt in/out from having third-party cookies placed in their computer. We evaluated these statements to be partial mapping since this is considered an indirect mapping as a user is never confronted with this knowledge unless one reads the privacy policies
rigorously (additional effort and reasoning is required). We found no corresponding opt in/out operation in the remaining sites.

V. DISCUSSION

We conducted these analyses using the privacy policies and privacy controls that were available to us during our data collection period. Given the nature of the data in the current study, we found that there were recurring changes to some of the social networking sites’ privacy policies and privacy controls from the time our data collection was performed. While this may cause minor changes to our categorisation and analysis we believe that our findings regarding the general state of privacy policy and privacy control disconnect, and the reasons for this disconnect, remain valid.

Our results show a significant lack of traceability between statements in privacy policies and the privacy controls of SNS. In total, two-thirds of the classified statements were evaluated as partial or broken (as illustrated in Fig. 2). Privacy policies do not provide explicit information enabling users to map policy fragments to the operations of SNS, thus contributing to lack of trust. Our analysis offers several observations and recommendations:

A. Overall lack of traceability

Our study shows that there is a widespread lack of traceability between privacy policies and the runtime implementation of privacy controls of SNS. In total only 23% of statements across all the surveyed sites could be categorised as having ‘complete’ traceability. The underlying causes here can be attributed to the SNS business model. As opposed to conventional service providers such as Amazon or Ebay where users are consumers/customers of the site, SNS users (and particularly their personal information) are the products themselves. SNS therefore generate their revenues based on sharing of users’ information with 3rd parties. This leads to an interesting dichotomy between the users’ privacy needs and the sustainability of the SNS service model - if everything were to be private then there would be no data on which to capitalise. However, the key question that our study raises is not that of an all or nothing privacy model. Instead it highlights the need for externally observable relationships between privacy policies and policy controls so that both users and SNS providers can have confidence that the latter are effective operationalisations of the former. This presents an interesting challenge for traceability and requirements engineering research - how can one provide such traceability in the presence of the often conflicting privacy and business needs in the open online social settings serviced by software in modern society.

B. Lack of transparency

Within our study, we traced the classified policy statements (based on actions) to the privacy controls using our mapping procedure (in Section III). We found that 43% of policy statements could not be mapped in any way to the available privacy controls, particularly when those statements related to actions that were non-optional with respect to the user –
such as indirect collection or aggregation of user activities. Unless a user is intimately familiar with the privacy policy, this can lead to a lack of user awareness of the way their data is being used which can in turn foster distrust. While this may not be seen as ‘broken’ by the SNS, the lack of transparency from the perspective of users can be traced to systemic failures on the part of the privacy policy. The interesting research challenge here is the need for effective privacy awareness mechanisms - whereby users can have a sense of how their actions are being monitored and utilised without compromising the usability of the SNS features. This in turn requires some tangible online experience to create and hone one’s sense of when one’s privacy is being compromised.

C. Indeterminable flow of information

Another interesting finding of our study is what we call ‘indeterminable flow of information’ – the problem of not being able to visualise and track the flow of one’s information through the SNS. This observation arose while performing content analysis on the privacy policies; when developing our classification for the sub-categories under our top-level action categories (i.e. Collection, Use, and Sharing) it became apparent that the kinds of data and visibility discussed under these top-level categories tend to be disconnected. For instance, consider this statement from Hi5’s privacy policy relating to collection: “If you send SMS, MMS, or text messages to the Services, we will collect the telephone number ...” In order to be able to easily track the flow of this information through the use and sharing stages we might expect corresponding references to this data under the appropriate use and sharing sections of the privacy policy; this is not however the case.

This highlights the need to have more effective structures for privacy policies that make the flow of information through the SNS from the collection stage to use and sharing more explicit. Furthermore, from a software design perspective, an interesting question to explore is whether the flow of information can be incorporated into the design of the privacy controls hence making such information flow visible during the users’ interactions with the privacy controls.

VI. CONCLUSION

We have presented a study examining the degree of traceability between privacy policies and privacy controls. We analysed externally observable relationships between the privacy policies and controls of 16 popular SNS. Our results reveal that the two-thirds of the principles addressed in the policies of SNS are not reflected in the runtime implementation of privacy controls that are presented to a user. These findings demonstrate that privacy management in the modern world, connected by innovative online social media, is a major issue. Researchers, social networking providers, privacy groups and users of social networking sites need to come together to address the key challenges exposed by our study, namely:

- How to balance the often conflicting economic and privacy goals of diverse stakeholders in an SNS – this requires new economic/business models for SNS that embrace privacy as a feature rather than an obstacle.
• How to make users more privacy-aware in their day-to-day interactions on SNS – this requires new modes of user experience in SNS that do not detract from the services offered by the SNS whilst providing a sense of ones exposure during interactions on an SNS.
• How to make information flow in SNS more transparent – this requires new forms of privacy controls that enable a user to understand what happens to his/her information when particular settings are selected. In other words, privacy policies should be transparently embodied into the privacy controls.

The study reported in this article is a stepping stone towards understanding these challenges. Establishing a clear traceability relationship will benefit both users (providing clearer guidance on how their information is handled) and SNS (validating the compliance exercise and increasing users’ trust). Note that a more formal description of our method, in which the degree of traceability between statements in the privacy policies and privacy controls of SNS can be systematically assessed, is presented in [12] which also illustrate the method’s wider applicability in other domains.

ACKNOWLEDGEMENTS

“Social Media, Social Good: Ultra-Large Scale Public Engagement Systems to Challenge Anti-Social Behaviour” This research is being funded by a Lancaster University 40th Anniversary Research Studentship, EPSRC Grant EP/I016546/1 and EP/I016546/1. We would also like to thank Barry Porter for his valuable feedback on this article.

REFERENCES


AUTHOR BIOS

Pauline Anthonysamy is a PhD student in the School of Computing and Communications at Lancaster University and is a member of the Cyber Security Research Centre at Lancaster University. Her research interests include developing computational approaches for privacy policy compliance and traceability to a system’s runtime functionality and the modelling and analysis of privacy in online social networks.

Phil Greenwood is a senior research associate in the School of Computing and Communications at Lancaster University and is a member of the Cyber Security Research Centre at Lancaster University. His research interests include the development of novel software engineering tools and techniques to address current and future cyber security risks whilst reconciling the associated social-technical challenges.

Awais Rashid is a Professor in the School of Computing and Communications at Lancaster University and co-director of the cross-disciplinary Security-Lancaster research centre. He also heads the EPSRC-GCHQ Academic Centre of Excellence in Cyber Security Research at Lancaster University. His relevant research interests include engineering trusted and trustworthy systems, socio-technical approaches to cyber security, privacy management and ethics. He is a member of the IEEE and IEEE Computer Society.
CONTACT INFORMATION

Miss. Pauline Anthonysamy,
Room C22, School of Computing and Communications,
Lancaster University, Infolab21,
Lancaster LA1 4WA, United Kingdom.
E-mail: anthonys@comp.lancs.ac.uk

Dr. Phil Greenwood
Room C22, School of Computing and Communications,
Lancaster University, Infolab21,
Lancaster LA1 4WA, United Kingdom.
E-mail: greenwop@comp.lancs.ac.uk

Prof. Awais Rashid
Room C41, School of Computing and Communications,
Lancaster University, Infolab21,
Lancaster LA1 4WA, United Kingdom.
E-mail: marash@comp.lancs.ac.uk