Learning to Share: Engineering Adaptive Decision-Support for Online Social Networks

How to cite:

For guidance on citations see FAQs.

© 2017 ACM

https://creativecommons.org/licenses/by-nc-nd/4.0/

Version: Accepted Manuscript

Link(s) to article on publisher’s website:
http://ase2017.org/

Copyright and Moral Rights for the articles on this site are retained by the individual authors and/or other copyright owners. For more information on Open Research Online's data policy on reuse of materials please consult the policies page.

oro.open.ac.uk
Abstract—Some online social networks (OSNs) allow users to define friendship-groups as reusable shortcuts for sharing information with multiple contacts. Posting exclusively to a friendship-group gives some privacy control, while supporting communication within this group. However, recipients of such posts may want to reuse content for their own social advantage, and can bypass existing controls by copy-pasting into a new post; this cross-posting poses privacy risks.

This paper presents a learning to share approach that enables the incorporation of more nuanced privacy controls into OSNs. Specifically, we propose a reusable, adaptive software architecture that uses rigorous runtime analysis to help OSN users to make informed decisions about suitable audiences for their posts. This is achieved by supporting dynamic formation of recipient-groups that benefit social interactions while reducing privacy risks. We exemplify the use of our approach in the context of Facebook.

I. INTRODUCTION

Online Social networks (OSNs) are increasingly used to maintain social ties with family members, friends, and colleagues, and build new social relationships (e.g., [1]–[3]). However, these benefits come with an increased risk of privacy violation from oversharing or underusing privacy controls [4]–[8]. Many OSN platforms currently support privacy management through features such as static (user-defined) friendship groups as reusable shortcuts for sharing a single post with multiple contacts. Users can select the group they deem most appropriate when posting a message. In OSNs such as Facebook, LinkedIn and Google+, users may perceive posting in closed group as a quick fix to their privacy concerns, since these OSNs can constrain the re-sharing to only those contacts who have received the original message. However, these privacy control mechanisms do not account for cross-posting, i.e. when a contact copy-and-pastes the original message into a new post, and sends it to contacts outside the original group.

In this paper, we propose an adaptive privacy control approach, called learning to share, that enables software engineers/developers to incorporate adaptive privacy decision support into OSN applications. Specifically, we propose a software architecture that supports continuous monitoring of online interactions between each user-contact pair in a user’s social network, to predict three categories of contacts: those who are most likely to pose a privacy breach (i.e., risky friends); those who are socially inactive but privacy aware (i.e., safe friends); and those who are both socially active and privacy aware (i.e., super friends). The prediction is based on an interaction model of sharing behaviours, which is updated on-line in response to monitored behaviour and used to evaluate social benefit and privacy risk of sharing a post with each potential recipient. The outcome of the classification is used by the decision support component of the architecture to dynamically form contacts lists per post, and allows the user to efficiently select the recipient group on a per post basis. The underlying OSN infrastructure can take into account the informed selection by the user and dynamically control who should be receiving which message when delivering the post.

Our proposed software architecture is not specific to a particular OSN environment. Software engineers working on developing and/or improving existing OSN applications with adaptive privacy decision mechanisms, can use our proposed architecture by deploying its automated learning and decision support capabilities, and integrating an Abstract Interaction Model and a wrapper for monitoring the type of social interactions that are specific to the particular OSN application.

The rest of the paper is organized as follows. Section II presents a motivating example within the context of Facebook. Section III describes our Learning to Share architecture. Section IV exemplifies how OSN behaviours can be modelled as parametric Markov model, using the example of Facebook; introduces the related component for monitoring social network activities, and presents the online learning algorithm used to predict the model’s parameters. Section V describes the computation of social benefit and privacy risk used by the
decision support component. Section VI discusses related work and concludes the paper with a summary and future work.

II. Motivating Example

Here, we illustrate the need for adaptive privacy control with a motivating example based on Facebook use. Facebook user Bob shares sensitive post A with his predefined close friends group, which does not include Ann – Bob’s work colleague but not a close friend. As Ann is not a member of the close friends group, Facebook does not allow her to see Bob’s post, and members of close friends are unable to re-share the post with her. Tom, a member of Bob’s close friends group, is also a close friend of Ann, but is unaware of this privacy aspect of Facebook’s group sharing. When Tom receives the post A, he naively decides to copy and paste the content into a new post, B, adding some content of his own, and shares B with a group of contacts which includes Ann. Now Ann can see, via cross-posting, what Bob shared in post A, but Facebook is unable to detect this or notify Bob that his on-line close friend Tom has violated his privacy, albeit unintentionally.

![Fig. 1: A scenario of privacy breach.](image)

This shows that, while customised social network groups are convenient for posting to multiple recipients and (in Facebook at least) offering a form of privacy control, this static feature can easily be bypassed, even fairly innocently. Good adaptive privacy control would, instead, monitor Tom’s actions, detect the similarity between posts A and B, and use this information to learn that sending sensitive posts to Tom represents a privacy risk, presenting this information to Bob the next time he intends to share another sensitive post with close friends.

III. Privacy Aware Sharing Architecture

Our proposed learning to share approach is implemented as a reusable, adaptive software architecture as shown in Figure 2. The architecture comprises two main modules: i) modelling and monitoring (marked C2), and ii) adaptive decision support (marked C3). This design enables software engineers working on OSN applications to deploy our architecture by reusing the automated learning and decision support capabilities and developing just two components: the abstract interaction model for the specific OSN application and a wrapper, which enables monitoring of the application specific social network interactions, and execution of sharing decisions.

The OSN wrapper implements the monitor functionality to detect for each recipient of each post subsequent interactions between user and recipient, e.g., resulting likes and comments on Facebook. Monitored events are used by the Learning Engine component, which updates the parameters of the associated instantiated interaction model, called Concrete Interaction Models, essentially capturing the probability of each possible social interaction at each post’s sensitivity level. The concrete interaction model is then queried by the Decision Support System (DSS) to assess sharing decisions. Specifically, the DSS employs the concrete interaction model, a risk averseness threshold and a post’s sensitivity level to evaluate the re-share risk and social benefit and to classify (at run-time) each of user’s contacts as super, safe or risky. Sensitivity levels of shared posts are defined by the user and stored, together with the post, to check for future re-shares of the post.

By providing just the wrapper and an abstract interaction model, learning to share can be deployed for different OSNs either as a fully integrated feature of an OSN’s infrastructure (i.e. total view mode), or as a plugin application of an existing OSN infrastructure (i.e. partial view mode). In the first case, the adaptive privacy control benefits from full access to the OSN’s global network community and the monitoring of online social behaviour of all members in the network. Whereas, partial view mode only provides adaptive privacy control and monitoring of users of the plugin application.

IV. Modelling and Monitoring Runtime Activity

This section describes the modelling module of our architecture as a parametric Markov model, illustrating it with an example of an abstract interaction model for Facebook. It also presents our online learning method for updating the model’s parameters and a method for monitoring social interaction events, used for computing the updates.

A. Quantitative Verification of Markov Chains

Online social interactions can be modelled using parametric Markov chains (PMC). These are defined as follows:

Definition 4.1: A reward-annotated finite state discrete-time parametric Markov chain (PMC), $M_t$, is the tuple
< S, s0, V, P, τ, L >, with S a finite set of states and initial state s0 ∈ S; V a set of real-valued parameters; P a parametric transition probability |S| × |S|-matrix whose elements are functions of V; the reward function τ: S → R≥0 assigning a non-negative reward for each state, and labelling function L: S → 2^AP assigning a set of atomic propositions to each state. The (i,j)th element of P, p_{ij}, is a function of parameters V (written p_{ij} ∈ F_V) and represents the probability of transitioning from s_i to s_j. p_{ij} takes values strictly in [0, 1] and \sum_j p_{ij} = 1 for all i.

Probabilistic model checker PRISM\textsuperscript{1}\cite{12} allows PMCs to be expressed in a high-level language, and efficiently evaluates queries expressed in a reward-extended version of probabilistic computational tree logic (PCTL)\cite{13}. We use PRISM’s reward query operator R_{=1}[\Phi] in conjunction with the reachability reward property \Phi = [ F a_i], to evaluate the average reward accumulated along a path until a state satisfying proposition a \in AP is reached (for PCTL semantics see [14]). When queried with a PMC, PRISM’s reward query operator produces a symbolic expression, V \in F_V, of the associated reward property (a function of V). In what follows we describe how we use this functionality to predict expected social benefit and privacy risk in the context of Facebook.

B. Modelling Sharing Behaviours

We describe here our PMC model for Facebook. It captures the online social interactions between a user and contact, c, following the user’s post. The first model, \mathcal{M}_c^1 (see Fig. 3) captures comments and likes from both contact c and the user following some post. This behaviour is assumed to be independent of a post’s sensitivity (as discussed later). States in \mathcal{M}_c^1 are: s_1, s_2, s_3 and s_4 respectively representing likes by c and user, and comments by c and user; initial state s_0; terminal state s_{end}; and s_6 that each execution must eventually make this transition, and this can happen at most once.

There are 5 remaining models, \mathcal{M}_{c,l}^2 (see Fig. 4), one per sensitivity level l \in \{0, 1, 2, 3, 4\}, which capture the reshare behaviour of the contact in response to a post at sensitivity l. States in \mathcal{M}_{c,l}^2 are: initial state s_0; terminal state s_{end}; and s_5 representing a reshare by c. \mathcal{M}_{c,l}^2 has two symbolic parameters q_l \in [0, 1] and r_4 ≥ 0. Again, transition probabilities, rewards and propositional labels are shown in the figure. In an example execution of \mathcal{M}_{c,l}^2 from state s_0, q_l is the probability that a c reshares, and this can happen at most once.

We wish to estimate the social benefit of all reactions which follow the user sharing a post at sensitivity l with c, and equate this with the total reward accumulated over the lifetime of the parallel execution of \mathcal{M}_c^1 and \mathcal{M}_{c,l}^2. This corresponds to the sum of the expressions returned by PRISM when R_{=1}[\Phi_{end}]

\sum_{i=1}^{4} p_{ij} r_i
\sum_{i=1}^{4} p_{ij} r_i (1 - \sum_{i=1}^{4} p_{ij})

We discuss the use of these expressions in Section V-A

|Fig. 3: PMC model of online social interactions between a Facebook user and their post recipient c.|

|Fig. 4: PMC model capturing the re-sharing behaviour of a recipient c for posts received with sensitivity level l.|

C. Online Learning of Sharing Behaviour

PMC modelling and analysis, like that described above, is conventionally used for offline analysis of system properties\cite{15},\cite{16}. We instead apply these techniques at runtime updating our PMC parameters in light of observed interactions. We must, however, consider two complicating factors. First, c’s behaviour may change with time, and so we use a variant of the adaptive Bayesian learning algorithm from\cite{17}. Secondly, we can never observe when the user-contact pair stop interacting on a given post. To address this, we account for unobserved transitions to terminal states, s_{end}, by noting that each execution must eventually make this transition, and constructing a synthetic observation to the end state for every shared post with the same time-stamp as the original share.

Here, we describe how transition probabilities p_{ij} of a PMC can be learned when the analysed system is operational, and its state transitions monitored (for Facebook these correspond to the monitored events, such as comments, likes, share and re-share). More formally, suppose that, we have observed K ≥ 0 transitions out of s_i ∈ S and that the k-th such transition 1 ≤ k ≤ K, is to state s_{j_k} ∈ S, we define

\sigma_{ij}^k = \begin{cases} 1 & \text{if } j_k = j \\ 0 & \text{otherwise} \end{cases}

\text{is invoked on each model. These queries can be invoked once at design time and respectively give:}

V_c^1 = \sum_{i=1}^{4} p_{ij} r_i
V_{c,l}^2 = q_l r_5

\text{We discuss the use of these expressions in Section V-A.

1Similar model checkers include MRMC\cite{10} and Ymer\cite{11}.
and estimate probability of a state transition from \( s_i \) to \( s_j \) as
\[
    p_{ij}^K = \frac{c_i^0}{c_i^0 + K} p_{ij}^0 + \frac{1}{c_i^0 + K} f_{ij}^K + g_{ij}^K
\]
where \( p_{ij}^0 \) is the prior for \( p_{ij}^K \), \( c_i^0 > 0 \) quantifies our confidence, \( f_{ij}^K \) and \( g_{ij}^K \) are defined recursively as:
\[
    f_{ij}^K = \alpha^{-(t_K - t_{K-1})} f_{ij}^{K-1} + \sigma_{ij}^K \\
    g_{ij}^K = \alpha^{-(t_K - t_{K-1})} g_{ij}^{K-1} + 1
\]
Here, \( t_K \) represents the timestamp of the \( K \)-th observation, and \( \alpha \geq 1 \) is an ageing parameter (see [17] for a full description and proof). These probability estimates have two key features: older observations are downweighted, allowing rapid adaptation to changes in \( p_{ij} \); and the recursive form means storage and computation complexity are both in \( O(1) \).

D. Interaction Monitoring

The Monitor component detects events that are being tracked by our behavioural models (see Section V-B), and, when detected, notifies the Learning Engine so that appropriate updates can be invoked (see Section IV-C). In order to detect cross-posting based on a post’s modality (e.g., text, image, audio or video), the Monitor component, state-of-the-art information retrieval techniques [18] can be implemented as a pluggable module to measure the similarity between posts sent to \( c \), and posts \( c \) subsequently shares with others. Posts that exceed some similarity threshold (e.g., [19]) can be treated as cross-posts and the Learning Engine notified. Such a task is becoming feasible recently with the advance of high performance hardware and also information retrieval techniques [19]–[25].

V. DECISION SUPPORT SYSTEM

In this section, we present the technical details of our decision support system (DSS) that elicits and models the sharing preferences of the user, and informs the user of any sharing decisions that represent significant benefits or exceed certain risk thresholds derived from these preferences. Section V-A and Section V-B formally define the social benefit and privacy risk models, and Section V-C describes how we initialise the parameters associated with these models. Finally, in Section V-D we discuss the mechanisms for the user to adjust the parameters of the privacy risk model, based on continual feedback about the working system from the user.

A. Social Benefit

The DSS estimates the social-benefit a user expects to gain when sharing a post with contact, \( c \), from the Concrete Interaction Models, described in Section IV-B. For our Facebook example, this is captured by models \( M_1^c \) and \( M_2^c \). These two models attribute socially-beneficial rewards to relevant social events: reshares (of non-sensitive posts), comments and likes by contact \( c \) and comments and likes in response by the user. A user may value each event differently, but for simplicity we assign a fixed value to each event type. As discussed in Section IV, the expected social-benefit for sharing a post with at sensitivity \( l \) with contact \( c \), is the expected total reward accumulated over the lifetime of the parallel computation of models \( M_1^c \) and \( M_2^c \), and is given by
\[
    B_{c,l} = V_1^c + V_2^c = \sum_{i=1}^{4} p_i r_i + q r_5
\]
For each potential sharing decision, the expected social benefit, \( B_{c,l} \), is compared to a threshold, \( B \), set for the user. If it exceeds that threshold, \( B_{c,l} > B \), then the user is notified by placing contact \( c \) in the super friends list. If a different behavioural model were implemented, then the above expression would need to be updated appropriately.

While a variety of choices could be made about rewards in our Facebook model, we suggest the following simple, intuitive choice. Without loss of generality, a contact’s comment is given a unitary reward, i.e. \( r_3 = 1 \). Other rewards \( r_1 = \frac{1}{2}, r_2 = \frac{1}{4}, r_4 = \frac{1}{4} \) and \( r_5 = 1 \) are based on a small study where participants were given a questionnaire about expected levels of interaction following a Facebook post.

B. Privacy Risk

The DSS also estimates privacy risk – a numerical value of undesirability related to risky decisions. By definition, sharing any post at sensitivity \( l = 0 \) carries no risk (reshares are desired). Sharing at higher sensitivity \( l > 0 \) with a contact \( c \) who has reshare probability \( q_{c,l} \), is considered a risky decision with associated risk
\[
    R_{c,l} = b \log_2(q_{c,l}) + a_l
\]
where \( 2^{q_{l}} \) is the damage value associated with a privacy breach (a known reshare) at sensitivity level \( l \), and \( b > 0 \) controls how risk averse the user is (their risk posture). When the user considers sharing a post of sensitivity \( l \) with \( c \), the associated risk, \( R_{c,l} \), is compared to the user’s risk-threshold, \( \bar{R} \). The DSS warns the user if \( R_{c,l} > \bar{R} \) by placing contact \( c \) into the risky list for that post. We define 5 sensitivity levels \( l = 0, 1, 2, 3, 4 \). For \( l > 0 \), \( a_l = l \) meaning a privacy breach at sensitivity \( l \) is half as damaging as one at \( l' = l + 1 \) (\( l = 0 \) means no risk).

Risk posture, \( b \), is set so \( R_{c,l} \) values, as closely as possible, reflect a user’s preferences over risky decisions. Risk appetite, \( \bar{R} \), represents the user’s maximum acceptable risk. These parameters are given initial values based on user input (Section V-C), then adjusted at runtime by the user (Section V-D).

C. Initialising Decision Support Parameters

As indicated, initial values for social benefit threshold, \( B \), risk-posture, \( b \), and risk-threshold, \( \bar{R} \), are elicited from users via a short, non-technical questionnaire, where they consider outcomes in three sharing scenarios. However, as a user may not feel able to respond to one or more questions, we provide null response options for each scenario, and generate default values based on previous responses.

\footnote{The questionnaire can be found at bit.ly/2x4Fqqs}
The social-benefit threshold, $\bar{B}$ aims to identify contacts who (on average) exceed a user’s expected level of social engagement. We quantify this as the expected number of likes, $N_l$, and comments, $N_c$, in response to a typical post from the user to 10 recipients, and use this to predict the expected social reward per person as:

$$\bar{B} = 0.1 \cdot (N_c + 0.5N_l) \quad (7)$$

The risk-posture, $b$, controls how the probability of a privacy breach affects the associated risk. Values of $0 < b < 1$ model risk-averseness, $b = 1$ models risk-neutrality and $b > 1$ models risk-seeking behaviour.

We elicit, $b$, indirectly from the user in terms of what we call the trade-probability, $\tilde{q}$ – the probability at which the user would trade exposure to two simultaneous privacy breaches for a guaranteed privacy breach, where all such privacy breaches are considered equally damaging. Risk posture is then calculated as:

$$b = \frac{-1}{\log_2(\tilde{q})} \quad (8)$$

The risk-threshold, $\bar{R} < 0$ (in conjunction with $b$) controls the regularity of warnings in the DSS. This value is again indirectly elicited, this time via the sensitivity 1 trigger probability, $\tilde{q}_1$ – the lowest probability of reshare for which the user would liked to be warned. The risk threshold is then calculated as:

$$\bar{R} = a_1 + b\log_2(\tilde{q}_1) = b\log_2(\tilde{q}_1) \quad (9)$$

Trigger probabilities at other sensitivity levels ($l > 0$) can then be calculated as: $\tilde{q}_l = \frac{2^{a_l-\bar{R}}}{1}$. 

D. Adjusting Decision Support Parameters

To provide additional user control over decision support, and to allow for poorly initialised values to be corrected for, we provide a mechanism to adjust risk-posture, $b$, and risk-threshold, $\bar{R}$, based on repeated contemporaneous judgements of the working system.

Adjusting $\bar{R}$: The lowest relevant sensitivity level, $l = 1$, has a maximum associated reshare risk of $0$ (see Equation (6)). Therefore $\bar{R}$ must be strictly negative, $\bar{R} < 0$. Otherwise, the user would never be warned at $l = 1$. We therefore propose multiplicative step adjustments to $\bar{R}$ with a fixed factor $\eta > 1$ to lower $\bar{R}$, and $\eta^{-1}$ to raise it. More precisely, if the user indicates that they have too many warnings, then we increase the threshold with: $\bar{R} \leftarrow \eta^{-1}\bar{R}$, which increases $\tilde{q}_l$ for all $l \geq 1$. Conversely, if the user indicates they are getting too few warnings then we reduce the threshold with: $\bar{R} \leftarrow \eta\bar{R}$.

Adjusting $b$: The risk-posture is also strictly positive, i.e. $b > 0$, so we again propose multiplicative changes by a new step factor, $\zeta > 1$. In our system, an increased risk-posture corresponds to a greater differentiation between sensitivity levels and vice versa. Therefore, the user can increase differentiation between sensitivity levels with an incremental increase in risk-averseness, effected with: $b \leftarrow \zeta b$. Similarly, a user can decrease this differentiation by decreasing risk-averseness, effected with: $b \leftarrow \zeta^{-1} b$. However, to ensure the baseline trigger probability $\tilde{q}_1$ remains unchanged, we also adjust the privacy threshold. So an increase in risk-averseness is accompanied by a reduction to the risk-threshold of: $\bar{R} \leftarrow \zeta\bar{R}$. Similarly, decrease in risk-averseness is accompanied by an increase to the risk-threshold of: $\bar{R} \leftarrow \zeta^{-1}\bar{R}$.

With these tools the user can incrementally shape the DSS system to suit their privacy preferences.

VI. RELATED WORK, CONCLUSION AND FUTURE WORK

A considerable body of research has been devoted to address the information sharing problem raised by the increasing number of privacy incidents and regrets happening in OSNs [8], [26]–[34]. However, these approaches do not consider the situation when users may have made poor sharing decisions in the past. Whereas, Machine learning and statistical inference approaches like [35]–[40] study information diffusion in OSNs in order to predict the temporal dynamics of the diffusion process. A very recent work [41] uses Inductive logic programming to build a formal model that learns users’ dynamic social identities at runtime in order to analyse group processes and intergroup relations in OSNs.

This paper presents a learning to share approach that enables software engineers/developers to readily add adaptive decision support to social network applications, such that the user has fine grained, informed control over their privacy settings. This allows users to maximise their social benefit, whilst controlling risk of privacy breaches to levels they find personally acceptable. We show how our approach can be used in the context of Facebook as the selected OSN platform. However the approach is applicable to other OSNs such as LinkedIn and Google+. This approach could also be readily extended to provide privacy control for a broader family of online interactions, such as undesirable cross-posting behaviours in social question answering services (e.g., StackOverflow) [42].

As for future work, we plan to conduct an online questionnaire in which users are asked to consider outcomes of their online sharing, based on scenarios discussed in Section V-C. This will help us to initialise the parameters of the DSS with realistic values. This will be followed by a user study to help us evaluate the feasibility of our approach from users’ perspective within the context of Facebook. For this purpose, a Facebook plug-in has been implemented and we are at the stage of designing and conducting the user study. Finally we will organise a workshop with OSN developers and present our learning to share architecture, implemented as Facebook plugin and the user study results. During this workshop we will collect qualitative feedback from developers and elicit their tendency towards integrating our approach as a privacy management for OSNs.

ACKNOWLEDGMENT

We would like to thank EPSRC, SFI and the ERC for their financial support.