“EVOLVING” PRIVACY POLICIES FOR SOCIAL NETWORKS

Gerardo Schneider
Dept. of Computer Science and Engineering
Chalmers | University of Gothenburg

Joint work with
Raúl Pardo, Christian Colombo, Ivana Kellyérová, & Gordon Pace

DRV’16
Bertinoro, 16-20 May 2016
## FACEBOOK PRIVACY SETTINGS

### Privacy Settings and Tools

<table>
<thead>
<tr>
<th>Who can see my stuff?</th>
<th>Who can see your future posts?</th>
<th>Friends</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review all your posts and things you're tagged in</td>
<td>Use Activity Log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limit the audience for posts you've shared with friends of friends or Public?</td>
<td>Limit Past Posts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who can contact me?</th>
<th>Who can send you friend requests?</th>
<th>Everyone</th>
<th>Edit</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Who can look me up?</th>
<th>Who can look you up using the email address you provided?</th>
<th>Friends</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who can look you up using the phone number you provided?</td>
<td></td>
<td>Friends</td>
<td>Edit</td>
</tr>
</tbody>
</table>

| Do you want search engines outside of Facebook to link to your profile? | Yes | Edit |

**What**

**Who**
Observation 1

Currently...

OSNs only allow to write *untimed static* (on/off) policies with a limited audience
<table>
<thead>
<tr>
<th>Who can look me up?</th>
<th>Who can contact me?</th>
<th>Who can see my stuff?</th>
<th>Who can see your friends?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- Do you want search engines outside of Facebook to link to your profile?
  - Yes

- Who provided your email address?
  - Friends

- How often?
  - Edit

FACEBOOK PRIVACY SETTINGS
FACEBOOK MESSENGER PRIVACY FLAW

Aran Khanna
May 26, 2015 · 6 min read

Stalking Your Friends with Facebook Messenger
FACEBOOK MESSENGER PRIVACY FLAW

“What you should keep in mind is that the mobile app for Facebook Messenger defaults to sending a location with all messages.”
A. Khanna

“[...] the latitude and longitude coordinates of the message locations have more than 5 decimal places of precision, making it possible to pinpoint the sender’s location to less than a meter.”
A. Khanna
FACEBOOK MESSENGER
PRIVACY FLAW

Interlude...
FACEBOOK’S REACTION

Three days later....

Facebook rescinds internship from student who exposed app privacy flaws

Harvard student Aran Khanna lost position after he launched app called Marauder’s Map that could pinpoint location of Facebook Messenger users

Stalking You

Facebook Messengers

Edit: At Facebook’s request I have removed the Mausoleum extension. Furthermore, Facemessenger, an earlier attempt to hack Facebook’s Messenger desktop webpage so the extension could access its data.
Observation 2

Trade off between

utility

(more functionality)

and

privacy
We would like...

OSNs allow to write *richer dynamic* ("evolving") *recurrent policies*

and that they are *properly enforced*
PRIVACY POLICIES

- [Audience] can know [some info] [more/less] times [X] times per [day/week/month/…]
PRIVACY POLICIES

My supervisor cannot see the pictures I’ve been tagged in during the weekend.

My supervisor cannot see my posts from 20:00 to 8:00.
POLICY AUTOMATA (1\textsuperscript{st} approach)

- Social Network event
- Timer
- A Boolean condition involving any element of the automaton or the OSN
- An update involving any element of the automaton or the OSN

A (\textit{static}) privacy policy
POLICY AUTOMATA - EXAMPLE

• Nobody can know my location more than 3 times per day

\[\text{post(location) \ \#location} < 3 \ \#\text{location}++\]

\[\text{post(location) \ \#location} == 3 \ \]

\[\text{@23:59 \ \#location} = 0\]
OTHER TIME PROPERTIES

• Nobody can know my location more than 3 times per day

For a given user, let’s say Martin

• After my location is posted 3 times, nobody can post it again within 24 hours
OTHER TIME PROPERTIES

- After my location is posted 3 times, nobody can post it again within 24 hours

```
post(location) \ #location < 3 \ #location++
```

```
post(location) \ #location == 3 \ c.reset()
```

```
c@24:00 \ \ #location = 0
```
IMPLEMENTATION (Prototype)

https://joindiaspora.com/
https://github.com/raulpardo/ppf-diaspora


* Joint work with R. Pardo, C. Colombo & G. Pace
What are you allowed to know?

- Nobody can know my location more than 3 times per day

The disclosure of this location should not be allowed...
Will Martin get to know this location?
Not at this moment! (According to the policy)

Martin could *learn* l4 later!
Observation 3

Defining (and enforcing) the right *dynamic recurrent privacy* policy is not easy

(Defining policy automata over *static* privacy policy languages gives more expressivity... but it’s not enough)
Real-Time Privacy Policies (2nd approach)

- Initial “time” (date)
- Duration
- Recurrence (hourly, daily, weekly, yearly)
- Agent

Restricted epistemic (knowledge) formula with real-time

Negation-free restricted epistemic (knowledge) formula with real-time

Bob cannot learn Alice location during weekends (starting Saturday April 16, 2016 at 00:00)

\[ [\neg L_{Bob\ location}(Alice)]_{Alice}^{[2016-04-16\ |\ 2\ days\ |\ 1\ week]} \]

* Ongoing joint work with R. Pardo & I. Kellyérová
ONGOING WORK...

• PPF: Privacy Policy Framework based on Epistemic Logic*
  • **Currently extending PPF with real-time** (R. Pardo & I. Kellyérová)

• **Policy automata**
  • Formal definition + simple properties - assuming a static privacy policy language (R. Pardo, C. Colombo & G. Pace)

• **Runtime enforcement of policy automata**
  • Prototype in Diaspora* using Larva (R. Pardo, C. Colombo & G. Pace)

FUTURE WORK and CHALLENGES

Combine real-time PPF with policy automata
• Expressiveness: e.g., geo-location privacy

Fully implement the framework (in Diaspora)
• Distributed monitors?
• Access control?

Automatic extraction of the enforcement mechanism from the framework
• Seems to need a full specification of all possible events from the OSN
TAKE AWAY

Currently...

Lack of rich “evolving” and recurrent privacy policies in OSNs
NEED OF...

Richer mechanisms to define and enforce “evolving and recurrent” privacy policies

Runtime Monitoring of Distributed Systems vs Distributed Runtime Monitoring

(Privacy Policies for multi-OSNs)
QUESTIONS?
DEMO

• [Nobody] can know [my location] more than [2X] times per [40/seconds]...
Definition 1. The tuple \( \langle SN, KBL_{SN}, \models, PPL_{SN}, \models_C \rangle \) is a privacy policy framework (denoted by \( \text{PPF} \)), where

- \( SN \) is a social network model;
- \( KBL_{SN} \) is a knowledge-based logic;
- \( \models \) is a satisfaction relation defined for \( KBL_{SN} \);
- \( PPL_{SN} \) is a privacy policy language;
- \( \models_C \) is a conformance relation defined for \( PPL_{SN} \).
PPF

\[ SN, u \models \neg p \quad \text{iff} \quad \neg p \in \nu(u) \]
\[ SN, u \models p \quad \text{iff} \quad p \in \nu(u) \]

\[ SN, u \models \neg \phi \quad \text{iff} \quad SN, u \not\models \phi \]
\[ SN, u \models \phi \land \psi \quad \text{iff} \quad SN, u \models \phi \text{ and } SN, u \models \psi \]

\[ SN, u \models K_i \delta \quad \text{iff} \quad \begin{cases} \delta \in KB(i) \text{ if } \delta = K_j \delta', \text{ where } j \in Ag \\ SN, i \models \delta \text{ otherwise} \end{cases} \]

\[ SN, u \models P^j_i a \quad \text{iff} \quad (i, j) \in A_a \]
\[ SN, u \models GP^j_G a \quad \text{iff} \quad (n, j) \in A_a \text{ for all } n \in G \]
\[ SN, u \models SP^j_G a \quad \text{iff} \quad \text{there exists } n \in G \text{ such that } (n, j) \in A_a \]

\[ SN, u \models S_G \delta \quad \text{iff} \quad \text{there exists } i \in G \text{ such that } SN, i \models K_i \delta \]
\[ SN, u \models E_G \delta \quad \text{iff} \quad SN, i \models K_i \delta \text{ for all } i \in G \]

\[ SN, u \models D_G \delta \quad \text{iff} \quad \begin{cases} SN, u \models S_G \delta' \text{ and } SN, u \models S_G \delta'' \text{ if } \delta = \delta' \land \delta'' \\ SN, u \models S_G \delta \text{ otherwise} \end{cases} \]

Table 1: $\mathcal{KBLC}_{SN}$ satisfiability relation
$SN \models_C \tau_1 \land \tau_2$ \quad iff \quad $SN \models_C \tau_1 \land SN \models_C \tau_2$

$SN \models_C [\neg \psi]_i$ \quad iff \quad $SN, i \models \neg \psi$

$SN \models_C [\phi \implies \neg \psi]_i$ \quad iff \quad $SN, i \models \phi$ then \quad $SN \models_C [\neg \psi]_i$

Table 2: $\mathcal{PPL}_{SN}$ conformance relation
Timed PPF

Fig. 1. Example of Timed Social Network Model
Timed PPF

\[
\begin{align*}
\sigma, t &\models \Box \varphi \quad \text{iff} \quad \text{for all } t' \in T_\sigma, t' \geq t, \sigma, t' \models \varphi \\
\sigma, t &\models \Diamond \varphi \quad \text{iff} \quad \text{there exists } t' \in T_\sigma, t' \geq t, \text{ such that } \sigma, t' \models \varphi \\
\sigma, t &\models \neg \varphi \quad \text{iff} \quad \sigma, t \not\models \varphi \\
\sigma, t &\models \varphi \land \psi \quad \text{iff} \quad \sigma, t \models \varphi \text{ and } \sigma, t \models \psi \\
\sigma, t &\models \forall x. \varphi \quad \text{iff} \quad \text{for all } v \in D_\sigma^{[t]}, \sigma, t \models \varphi[v/x] \\
\sigma, t &\models c_m(i, j) \quad \text{iff} \quad (i, j) \in C_m^{[t]} \\
\sigma, t &\models a_n(i, j) \quad \text{iff} \quad (i, j) \in A_n^{[t]} \\
\sigma, t &\models p(s) \quad \text{iff} \quad \text{there exists } t' \in T_\sigma, t' \leq t, \text{ such that } (p(s), t') \in KB_e^{[t]} \\
\sigma, t &\models K_i \varphi \quad \text{iff} \quad \text{there exists } t' \in T_\sigma, t' \leq t, \text{ such that } (\varphi, t') \in Cl_t(KB_i^{[t]}) \\
\sigma, t &\models L_i \varphi \quad \text{iff} \quad (\varphi, t) \in Cl_t(KB_i^{[t]}) \\
\sigma, t &\models C_G \varphi \quad \text{iff} \quad \sigma, t \models E_G^k \varphi \text{ for } k = 1, 2, \ldots \\
\sigma, t &\models D_G \varphi \quad \text{iff} \quad \text{there exists } t' \in T_\sigma, t' \leq t, \text{ such that } (\varphi, t') \in Cl_t(\bigcup_{i \in G} KB_i^{[t]})
\end{align*}
\]

Table 1. The Satisfiability Relation for $\mathcal{TKBL}_{SN}$
Timed PPF

\[ \sigma \models C \delta_1 \land \delta_2 \quad \text{iff} \quad \sigma \models C \delta_1 \land \sigma \models C \delta_2 \]

\[ \sigma \models C \forall x.\delta \quad \text{iff for all } v \in D_\sigma^{[t]} , \sigma \models C \delta[v/x] \]

\[ \sigma \models C [\neg \alpha]^i_{s+d|r} \quad \text{iff for all positive } c \in \mathbb{Z} \text{ such that } 0 \leq s + cr \leq \max(T_\sigma) , \]

\[ \sigma \models C [\neg \alpha]^i_{s+cr+d} \]

\[ \sigma \models C [\neg \alpha]^i_{s+d} \quad \text{iff } \sigma[s..s+d], s \models \Box(\neg \alpha) \]

\[ \sigma \models C [\neg \alpha]^i_{s} \quad \text{iff } \sigma[s..], s \models \Box(\neg \alpha) \]

\[ \sigma \models C [\varphi \implies \neg \alpha]^i_{s+d|r} \quad \text{iff for all positive } c \in \mathbb{Z} \text{ such that } 0 \leq s + cr \leq \max(T_\sigma) , \]

\[ \sigma \models C [\varphi \implies \neg \alpha]^i_{s+cr+d} \]

\[ \sigma \models C [\varphi \implies \neg \alpha]^i_{s+d} \quad \text{iff } \sigma[s..s+d], s \models \Box(\varphi \implies \neg \alpha) \]

\[ \sigma \models C [\varphi \implies \neg \alpha]^i_{s} \quad \text{iff } \sigma[s..], s \models \Box(\varphi \implies \neg \alpha) \]

**Table 3. The Conformance Relation for T\mathcal{P}\mathcal{P}\mathcal{L}_{SN}**