"THE NEXT GENERATION" PRIVACY POLICIES FOR SOCIAL NETWORKS

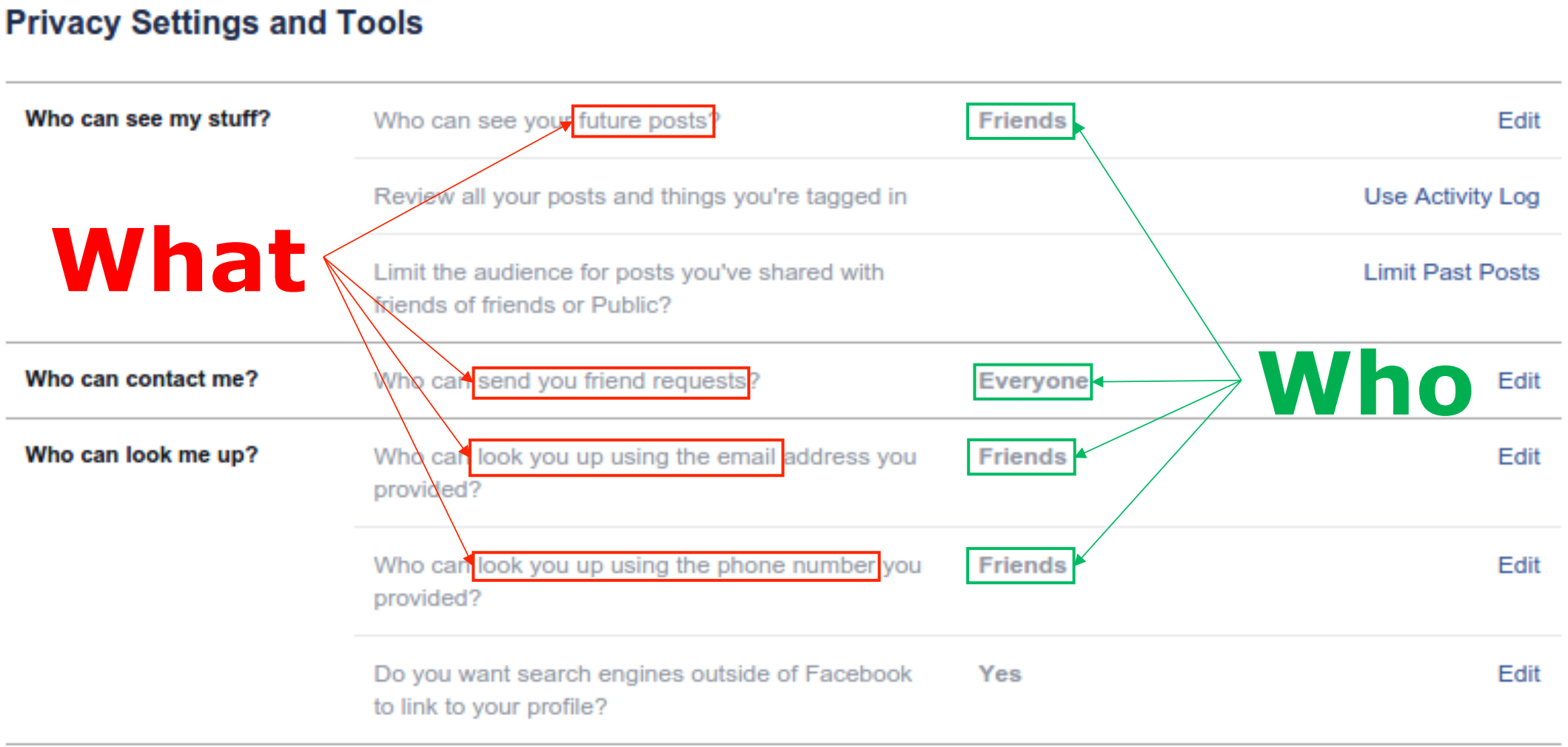
Gerardo Schneider
Dept. of Computer Science and Engineering
Chalmers | University of Gothenburg

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

UNIVERSITY OF
GOTHENBURG

DRV'16
Bertinoro, 16-20 May 2016

FACEBOOK PRIVACY SETTINGS

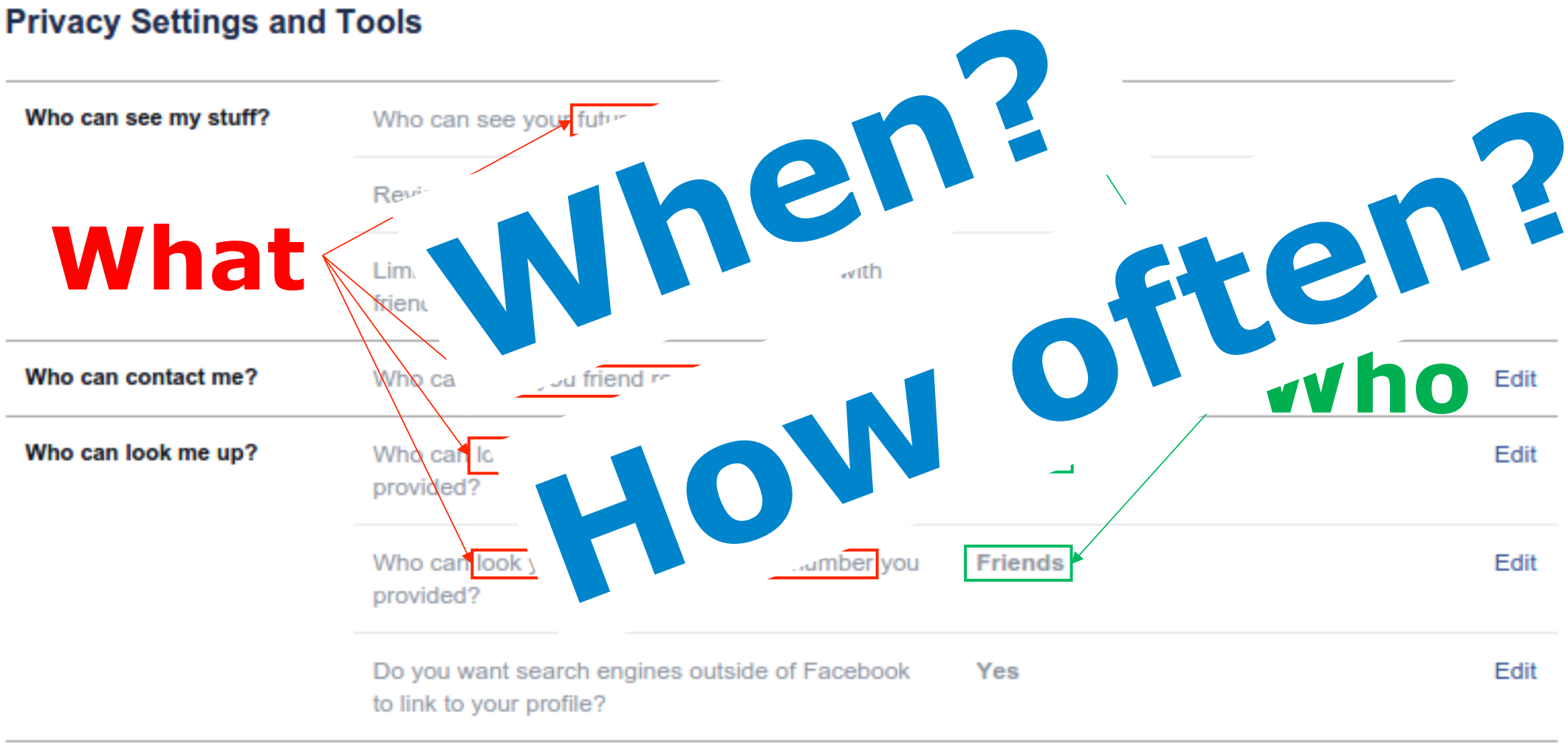


Observation 1

Currently…

OSNs *only* allow to write *untimed static* (on/off) policies with a limited audience

FACEBOOK PRIVACY SETTINGS



Interlude…

FACEBOOK MESSENGER PRIVACY FLAW

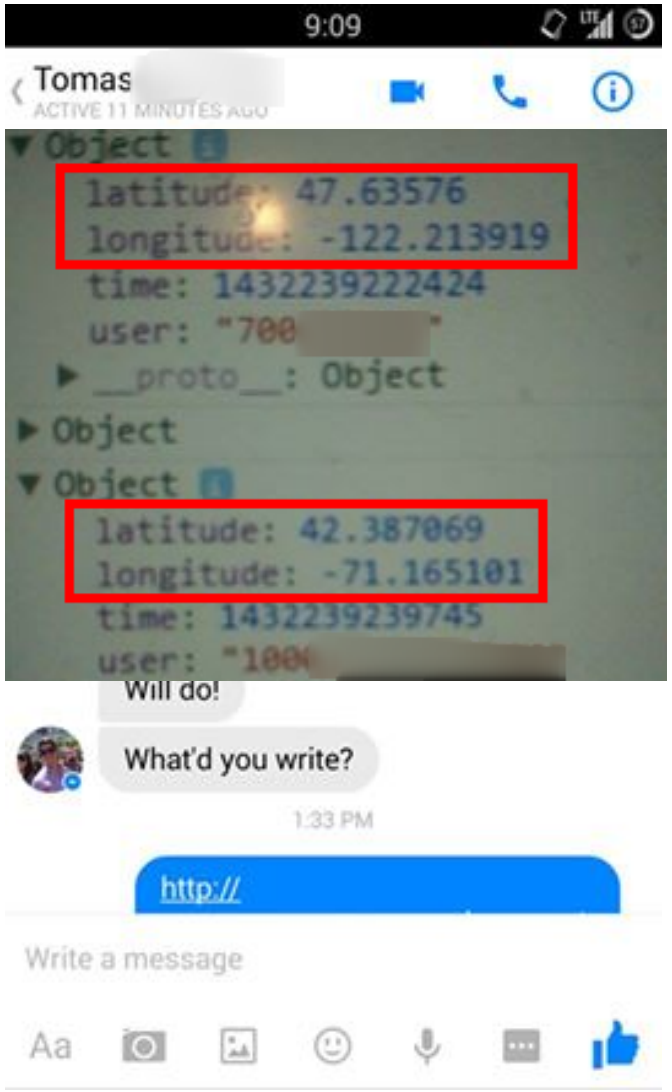
Aran Khanna
May 26, 2015 · 6 min read

Stalking Your Friends with Facebook Messenger

FACEBOOK MESSENGER PRIVACY FLAW

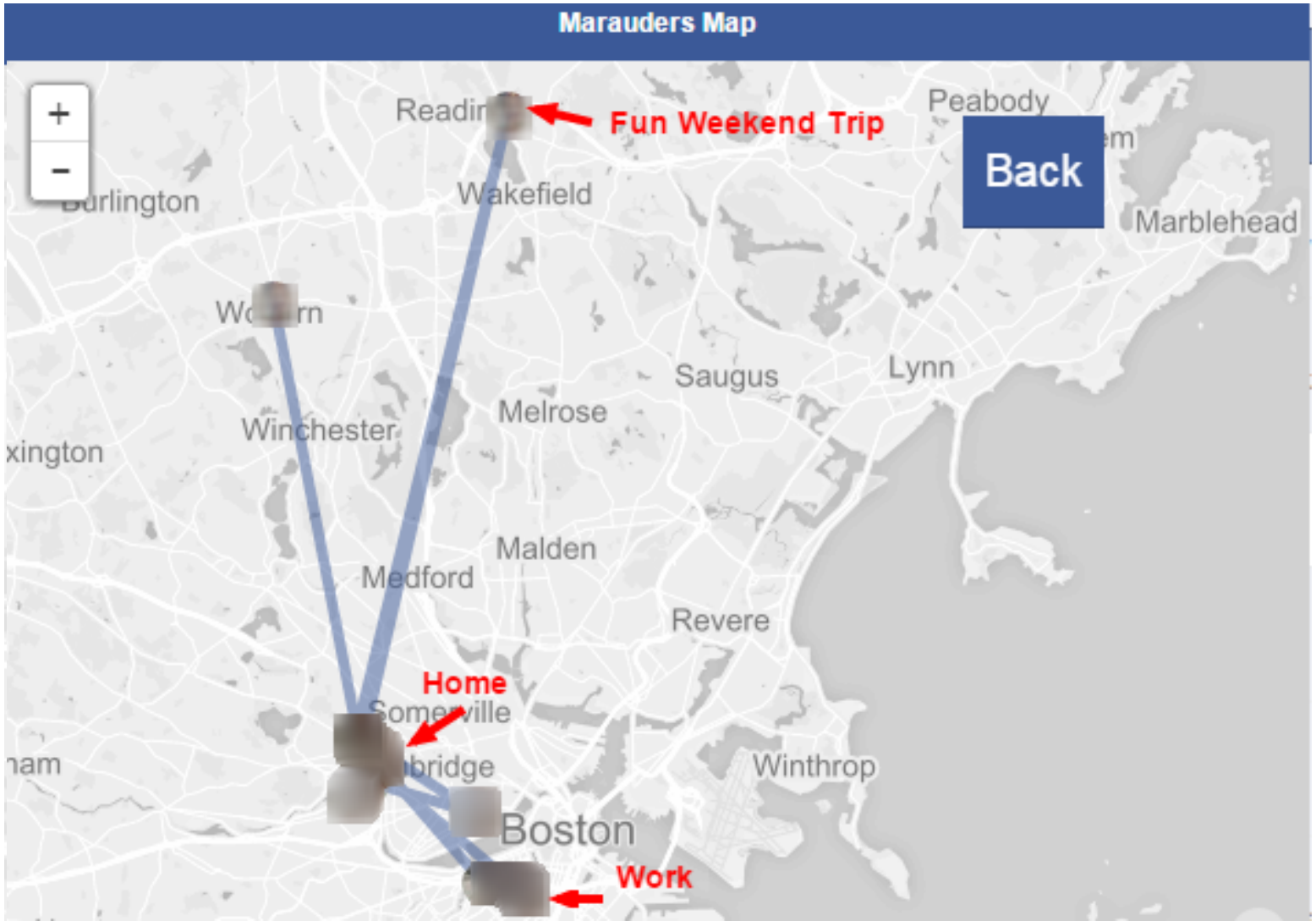
"What you should keep in mind is that the mobile app for Facebook Messenger **defaults** to sending a location with **all** messages."
A. Khanna

"[…] 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



Interlude…

FACEBOOK MESSENGER PRIVACY FLAW



FACEBOOK'S REACTION

Three days later….

Aran Khanna
May 26, 2015 · 6 min read

Stalking You
Facebook M

Edit: At Facebook's request I h
extension. Furthermore, Facel
desktop webpage so the exten

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

Observation 2

Trade off between

utility

(more functionality)

and

privacy

We would like…

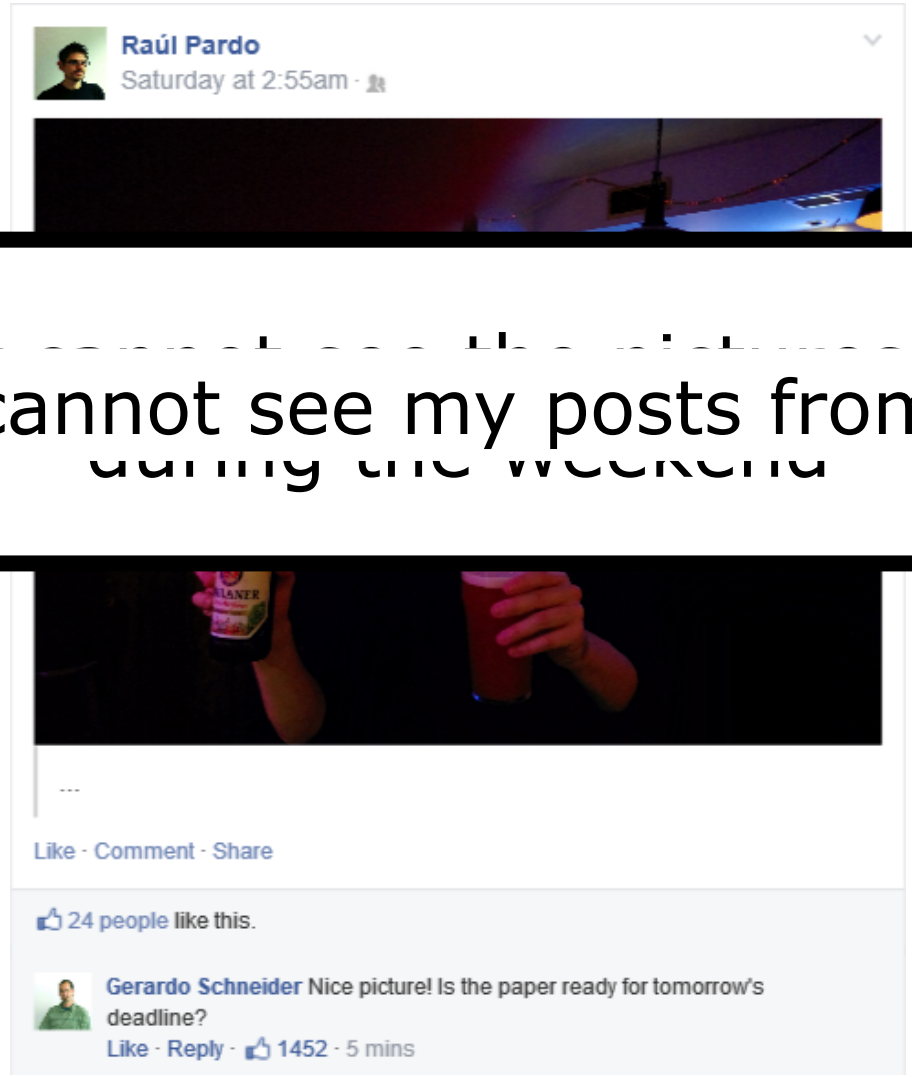
OSNs allow to write *richer* *dynamic* (*"evolving"*) *recurrent* policies

and that they are *properly enforced*

PRIVACY POLICIES

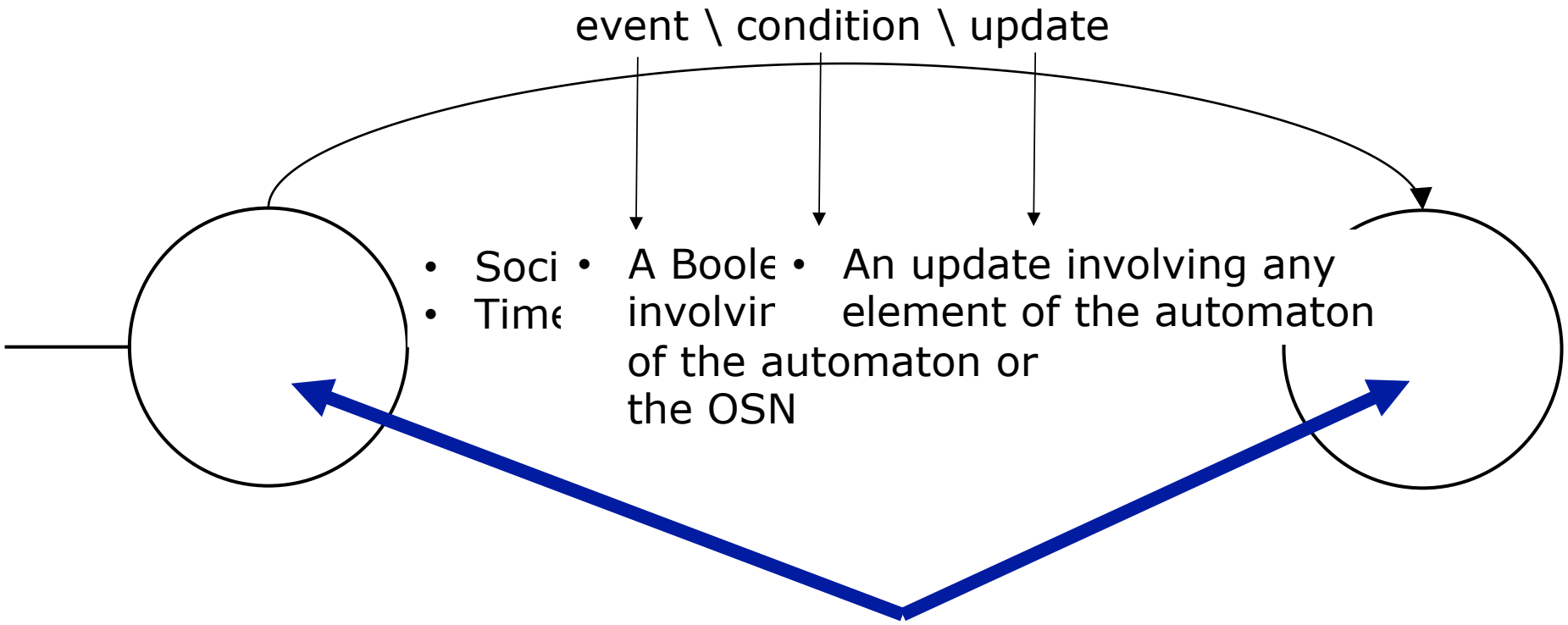
- [Audience] can know [some info] [more/less] [X] [day/week/month/…]

PRIVACY POLICIES



My supervisor cannot see my posts from 20:00 to 8:00

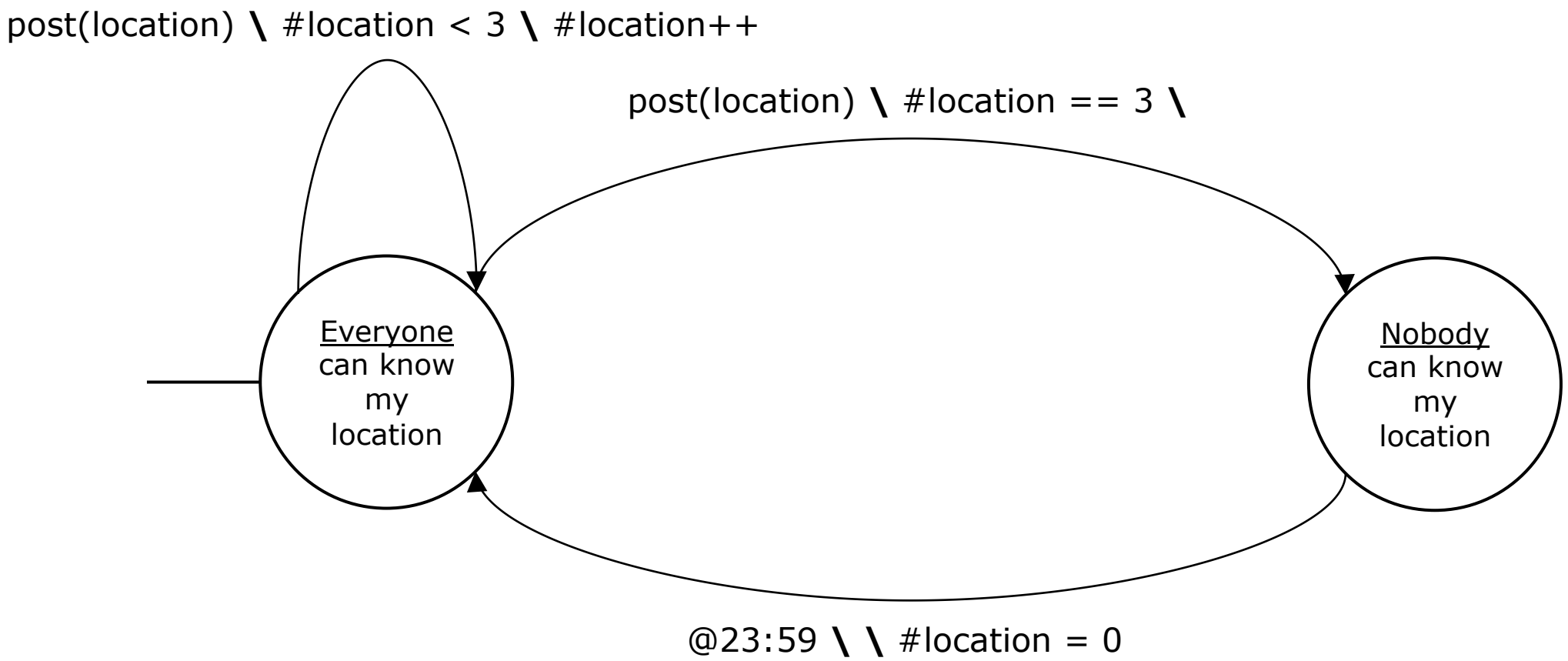
POLICY AUTOMATA (1st approach)



A (*static*) privacy policy

POLICY AUTOMATA - EXAMPLE

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



OTHER TIME PROPERTIES

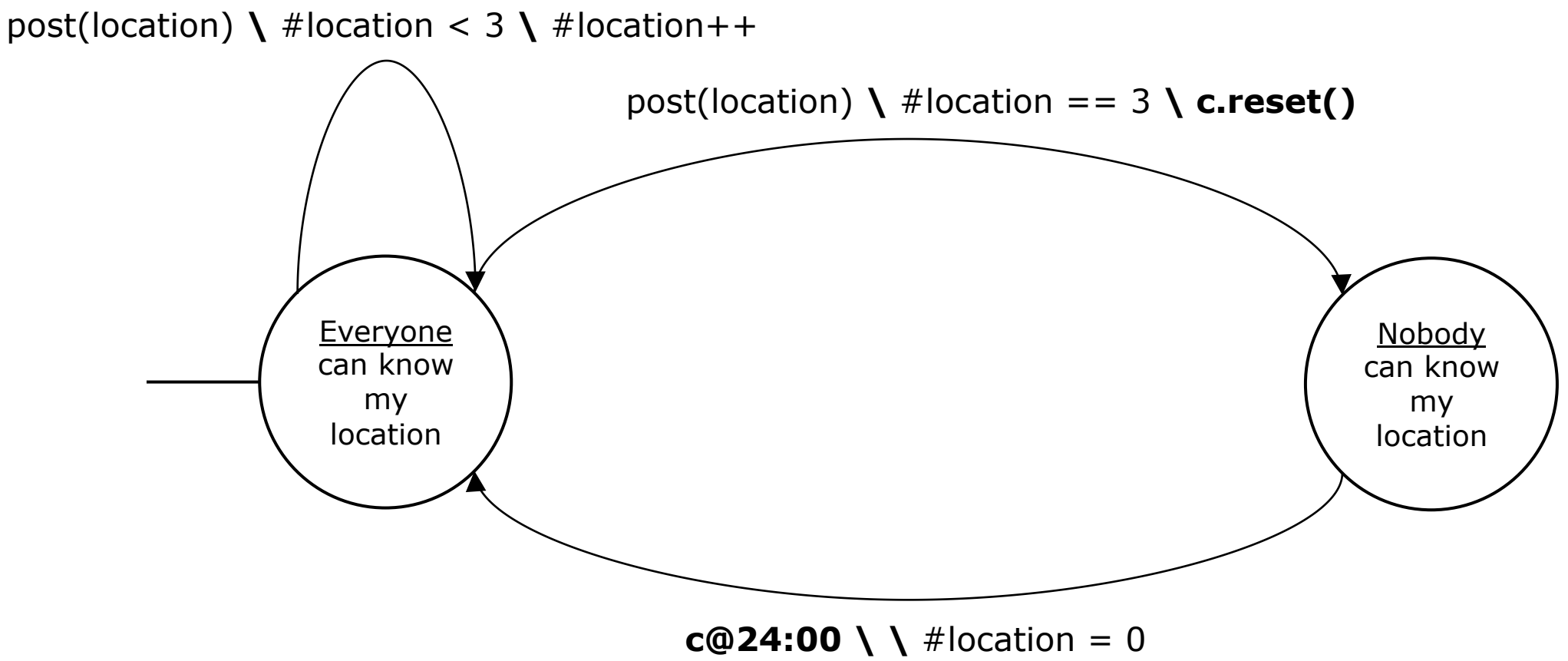
- Nobody can know my location more than 3 times per day

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

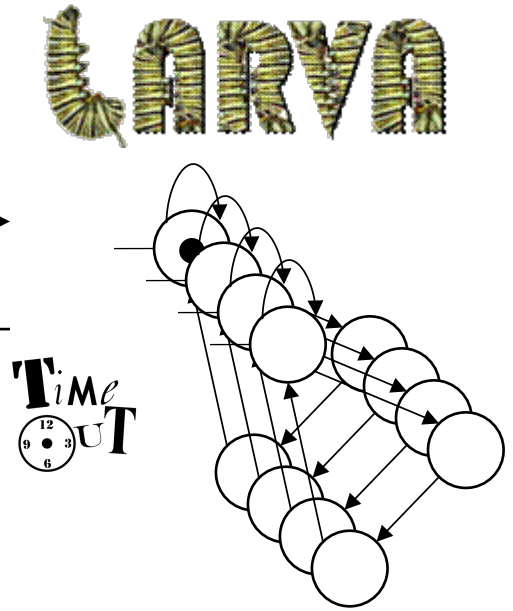
- After my location is posted 3 times, nobody can post it again within 24 hours



IMPLEMENTATION (Prototype)

event

ψ



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

http://www.cs.um.edu.mt/svrg/Tools/LARVA/

* 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)

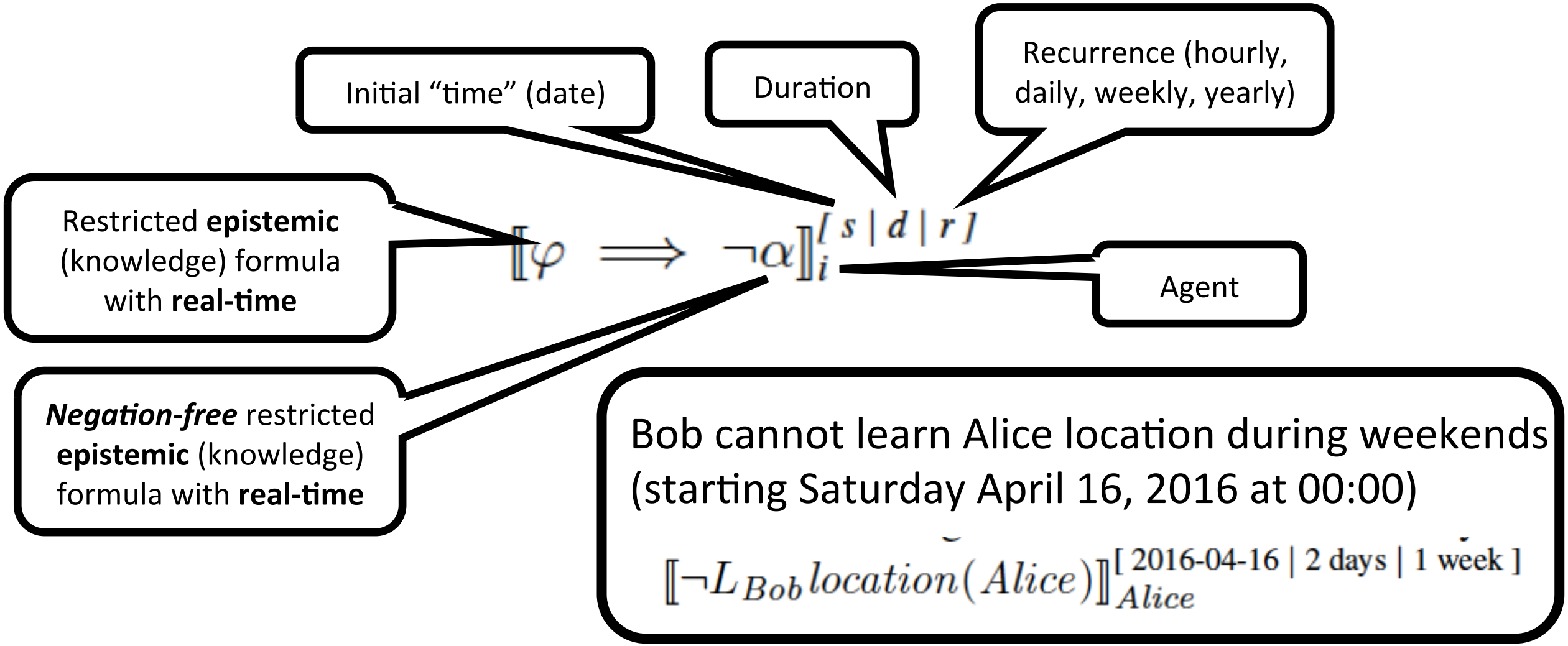
Martin could ***learn*** l4 **later**!

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)



* 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)

* R. Pardo & G. Schneider. *A formal privacy policy framework for social networks.* In SEFM'14, LNCS vol.8702, pp.378-392, 2014

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 [day/week/month/...]

PPF

Definition 1. *The tuple* $\langle \mathcal{SN}, \mathcal{KBL}_{\mathcal{SN}}, \models, \mathcal{PPL}_{\mathcal{SN}}, \models_C \rangle$ *is a* privacy policy framework *(denoted by* $\mathcal{PPF}$*), where*

- $\mathcal{SN}$ *is a social network model;*
- $\mathcal{KBL}_{\mathcal{SN}}$ *is a knowledge-based logic;*
- $\models$ *is a satisfaction relation defined for* $\mathcal{KBL}_{\mathcal{SN}}$*;*
- $\mathcal{PPL}_{\mathcal{SN}}$ *is a privacy policy language;*
- $\models_C$ *is a conformance relation defined for* $\mathcal{PPL}_{\mathcal{SN}}$*.* □

PPF

$$
\begin{array}{ll}
SN, u \models \neg p & \text{iff } \neg p \in \nu(u) \\
SN, u \models p & \text{iff } p \in \nu(u)
\end{array}
$$

$$
\begin{array}{ll}
SN, u \models \neg\phi & \text{iff } SN, u \not\models \phi \\
SN, u \models \phi \wedge \psi & \text{iff } SN, u \models \phi \text{ and } SN, u \models \psi
\end{array}
$$

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

$$
\begin{array}{ll}
SN, u \models P_i^j a & \text{iff } (i,j) \in A_a \\
SN, u \models GP_G^j a & \text{iff } (n,j) \in A_a \text{ for all } n \in G \\
SN, u \models SP_G^j a & \text{iff there exits } n \in G \text{ such that } (n,j) \in A_a
\end{array}
$$

$$
\begin{array}{ll}
SN, u \models S_G\delta & \text{iff there exits } i \in G \text{ such that } SN, i \models K_i\delta \\
SN, u \models E_G\delta & \text{iff } SN, i \models K_i\delta \text{ for all } i \in G
\end{array}
$$

$$
SN, u \models D_G\delta \quad \text{iff} \quad \begin{cases} SN, u \models S_G\delta' \text{ and } SN, u \models S_G\delta'' & \text{if } \delta = \delta' \wedge \delta'' \\ SN, u \models S_G\delta & \text{otherwise} \end{cases}
$$

Table 1: $\mathcal{KBL}_{\mathcal{SN}}$ satisfiability relation

PPF

$SN \models_C \tau_1 \wedge \tau_2$	iff $SN \models_C \tau_1 \wedge SN \models_C \tau_2$
$SN \models_C [\![\neg\psi]\!]_i$	iff $SN, i \models \neg\psi$
$SN \models_C [\![\phi \implies \neg\psi]\!]_i$	iff $SN, i \models \phi$ then $SN \models_C [\![\neg\psi]\!]_i$

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

Timed PPF

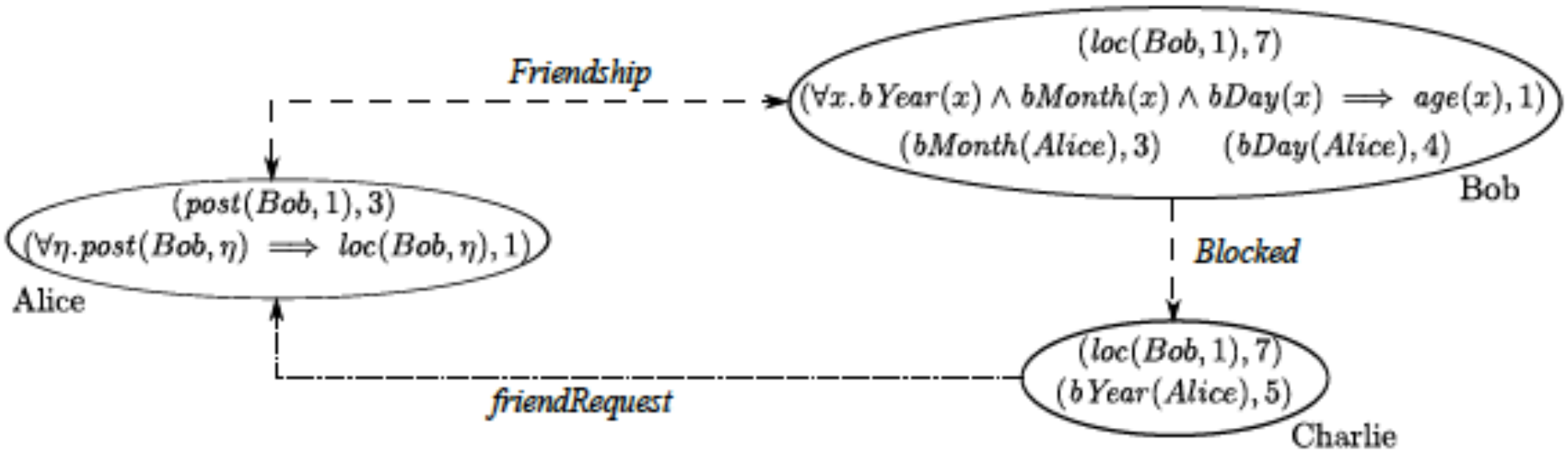


Fig. 1. Example of Timed Social Network Model

Timed PPF

$\sigma, t \models \Box\varphi$	iff	for all $t' \in \mathbb{T}_\sigma, t' \geq t, \sigma, t' \models \varphi$
$\sigma, t \models \Diamond\varphi$	iff	there exists $t' \in \mathbb{T}_\sigma, t' \geq t$, such that $\sigma, t' \models \varphi$
$\sigma, t \models \neg\varphi$	iff	$\sigma, t \not\models \varphi$
$\sigma, t \models \varphi \wedge \psi$	iff	$\sigma, t \models \varphi$ and $\sigma, t \models \psi$
$\sigma, t \models \forall x.\varphi$	iff	for all $v \in D_o^{\sigma[t]}, \sigma, t \models \varphi[v/x]$
$\sigma, t \models c_m(i, j)$	iff	$(i, j) \in C_m^{\sigma[t]}$
$\sigma, t \models a_n(i, j)$	iff	$(i, j) \in A_n^{\sigma[t]}$
$\sigma, t \models p(\vec{s})$	iff	there exists $t' \in \mathbb{T}_\sigma, t' \leq t$, such that $(p(\vec{s}), t') \in KB_e^{\sigma[t]}$
$\sigma, t \models K_i\varphi$	iff	there exists $t' \in \mathbb{T}_\sigma, t' \leq t$, such that $(\varphi, t') \in Cl_t(KB_i^{\sigma[t]})$
$\sigma, t \models L_i\varphi$	iff	$(\varphi, t) \in Cl_t(KB_i^{\sigma[t]})$
$\sigma, t \models C_G\varphi$	iff	$\sigma, t \models E_G^k\varphi$ for $k = 1, 2, \ldots$
$\sigma, t \models D_G\varphi$	iff	there exists $t' \in \mathbb{T}_\sigma, t' \leq t$, such that $(\varphi, t') \in Cl_t(\bigcup_{i \in G} KB_i^{\sigma[t]})$

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

Timed PPF

$\sigma \models_C \delta_1 \wedge \delta_2$	iff $\sigma \models_C \delta_1 \wedge \sigma \models_C \delta_2$
$\sigma \models_C \forall x.\delta$	iff for all $v \in D_o^{\sigma[t]}$, $\sigma \models_C \delta[v/x]$
$\sigma \models_C [\![\neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}\,\vert\,\mathbf{d}\,\vert\,\mathbf{r}]}$	iff for all positive $c \in \mathbb{Z}$ such that $0 \leq s + cr \leq \max(\mathbb{T}_\sigma)$, $\sigma \models_C [\![\neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}+\mathbf{cr}\,\vert\,\mathbf{d}]}$
$\sigma \models_C [\![\neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}\,\vert\,\mathbf{d}]}$	iff $\sigma[s \,..\, s+d], s \models \Box(\neg\alpha)$
$\sigma \models_C [\![\neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}]}$	iff $\sigma[s \,..\,], s \models \Box(\neg\alpha)$
$\sigma \models_C [\![\varphi \implies \neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}\,\vert\,\mathbf{d}\,\vert\,\mathbf{r}]}$	iff for all positive $c \in \mathbb{Z}$ such that $0 \leq s + cr \leq \max(\mathbb{T}_\sigma)$, $\sigma \models_C [\![\varphi \implies \neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}+\mathbf{cr}\,\vert\,\mathbf{d}]}$
$\sigma \models_C [\![\varphi \implies \neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}\,\vert\,\mathbf{d}]}$	iff $\sigma[s \,..\, s+d], s \models \Box(\varphi \implies \neg\alpha)$
$\sigma \models_C [\![\varphi \implies \neg\alpha]\!]_{\mathbf{i}}^{[\mathbf{s}]}$	iff $\sigma[s \,..\,], s \models \Box(\varphi \implies \neg\alpha)$

Table 3. The Conformance Relation for $\mathcal{TPPL}_{\mathcal{SN}}$