A FORMAL FRAMEWORK FOR PRIVACY POLICIES

GERARDO SCHNEIDER
Dept. of Computer Science and Engineering

(Joint work with **RAÚL PARDO*** and **MUSARD BALLIU**)

CHALMERS

UNIVERSITY OF
GOTHENBURG

Nijmegen, 27 June 2015

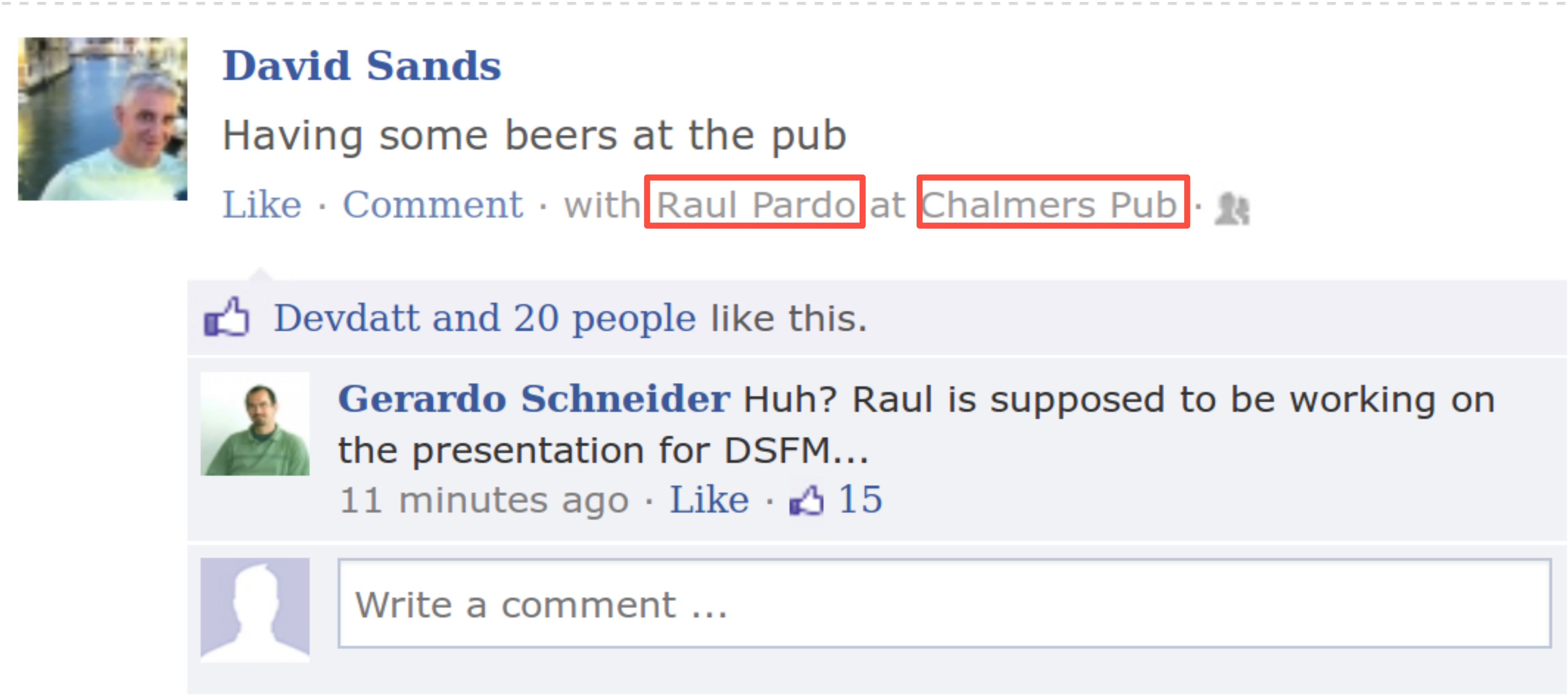
* Thanks to Raúl for some of the slides

OUTLINE

Part I: About privacy policies on Social Network Systems (SNS)

Part II: A very brief summary of other research interests

MOTIVATION



David Sands

Having some beers at the pub

Like · Comment · with Raul Pardo at Chalmers Pub ·

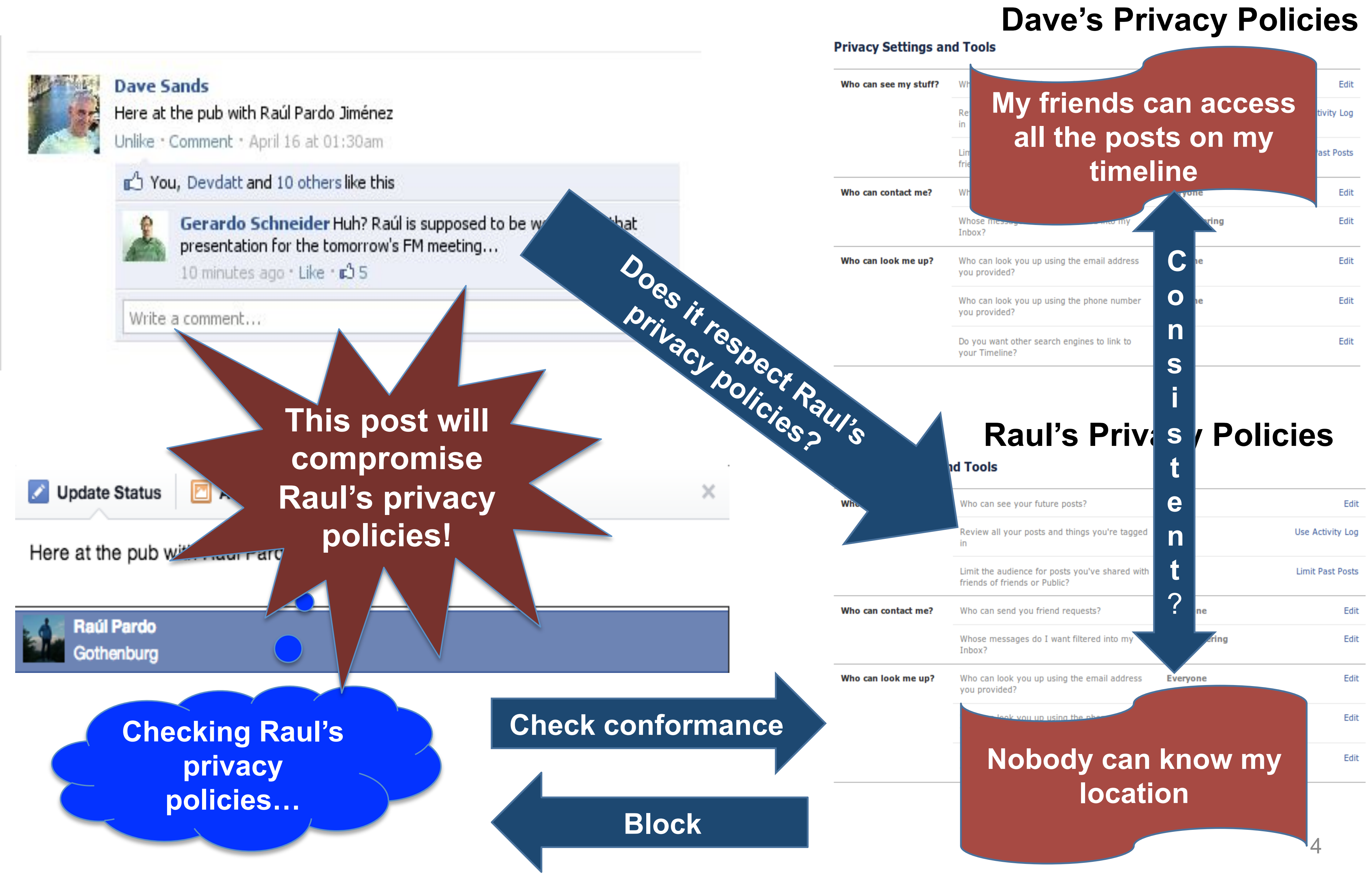
Devdatt and 20 people like this.

Gerardo Schneider Huh? Raul is supposed to be working on the presentation for DSFM...

11 minutes ago · Like · 15

Write a comment ...

MOTIVATION



Dave Sands
Here at the pub with Raúl Pardo Jiménez
Unlike · Comment · April 16 at 01:30am

You, Devdatt and 10 others like this

Gerardo Schneider Huh? Raúl is supposed to be w hat presentation for the tomorrow's FM meeting...
10 minutes ago · Like · 5

Write a comment...

This post will compromise Raul's privacy policies!

Update Status
Here at the pub wi Raul Pard
Raúl Pardo
Gothenburg

Checking Raul's privacy policies…

Check conformance

Block

Does it respect Raul's privacy policies?

Dave's Privacy Policies

Privacy Settings and Tools

Who can see my stuff? Wh Edit
Re in tivity Log
Lin frie ast Posts
Who can contact me? Wh yone Edit
Whose messag into my Inbox? ring Edit
Who can look me up? Who can look you up using the email address you provided? ne Edit
Who can look you up using the phone number you provided? ne Edit
Do you want other search engines to link to your Timeline? Edit

My friends can access all the posts on my timeline

Consistent?

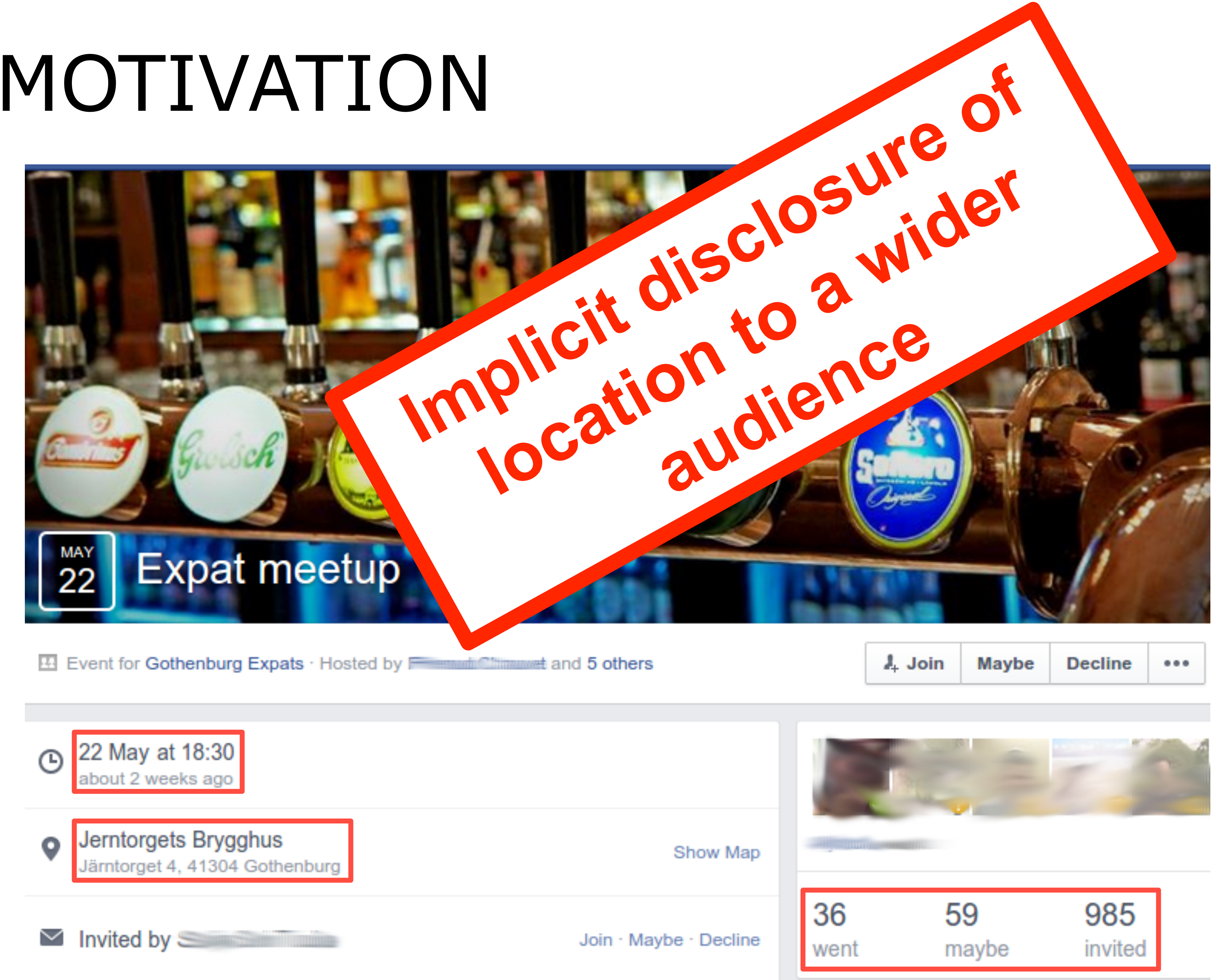
Raul's Priva y Policies

nd Tools

Wh Who can see your future posts? Edit
Review all your posts and things you're tagged in Use Activity Log
Limit the audience for posts you've shared with friends of friends or Public? Limit Past Posts
Who can contact me? Who can send you friend requests? ne Edit
Whose messages do I want filtered into my Inbox? ering Edit
Who can look me up? Who can look you up using the email address you provided? Everyone Edit
look you up using the pho Edit
Edit

Nobody can know my location

MOTIVATION



Implicit disclosure of location to a wider audience

MAY 22 Expat meetup

Event for Gothenburg Expats · Hosted by [redacted] and 5 others

22 May at 18:30
about 2 weeks ago

Jerntorgets Brygghus
Järntorget 4, 41304 Gothenburg

Show Map

Invited by [redacted]

Join · Maybe · Decline

[redacted]

36 went

59 maybe

985 invited

PRIVACY POLICIES IN SNS TODAY

- Limited expressivity on what you can write
- Conformance partially supported in many social networks
  - But limited: no analysis of (post) content, side effects of events (tagging, joining an event, etc.)
- Consistency among policies
  - Not supported in general…
  - Even less among multiple SNS

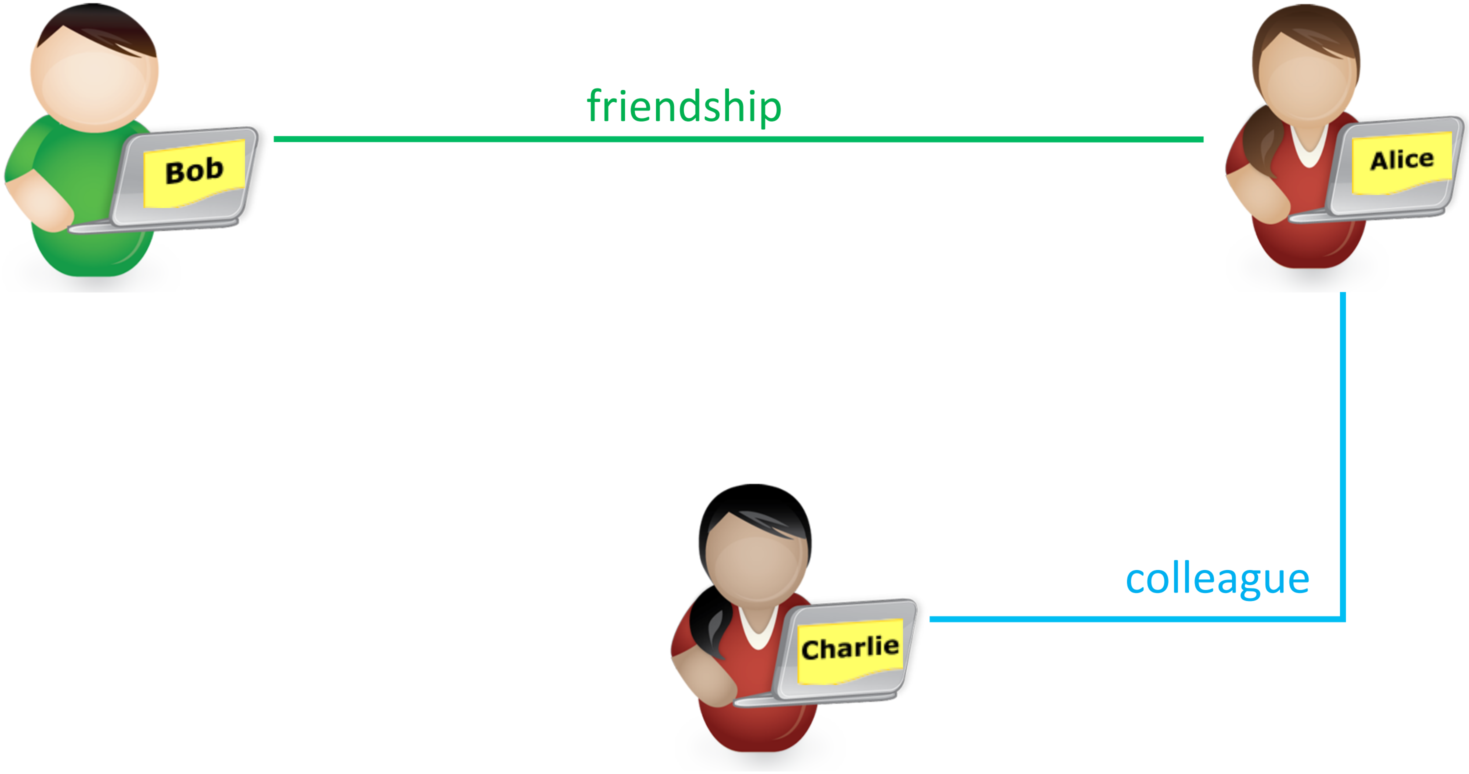
OUR (MID-TERM) GOAL

- Define a privacy policy framework allowing to write rich privacy policies for social networks
  - Beyond current SNS like
  - Beyond a single SNS

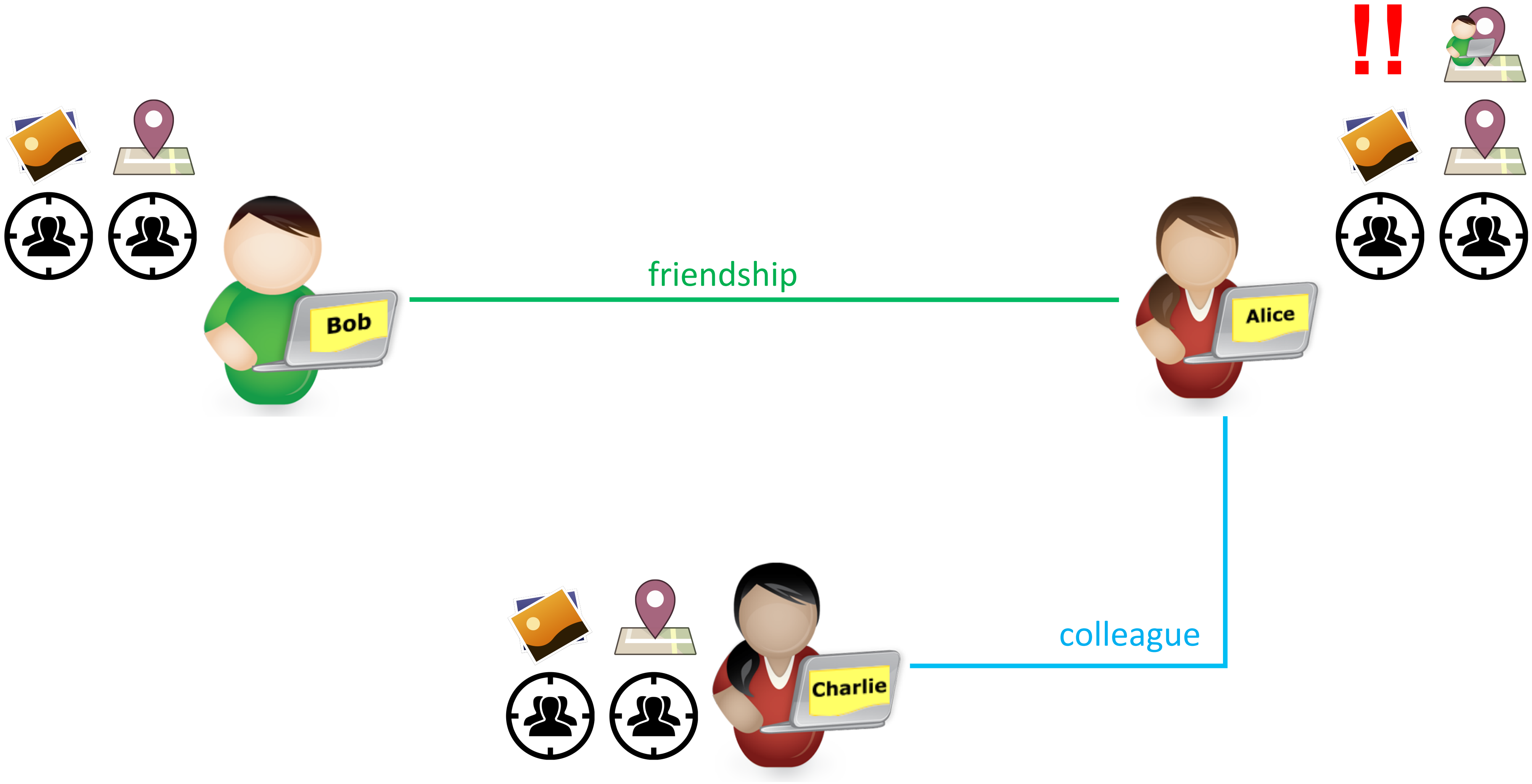
- Means for reasoning about properties of such policies (and the SNS)
  - Model checking, deductive system,…
  - Implicit and explicit knowledge

- Provide enforcement mechanisms

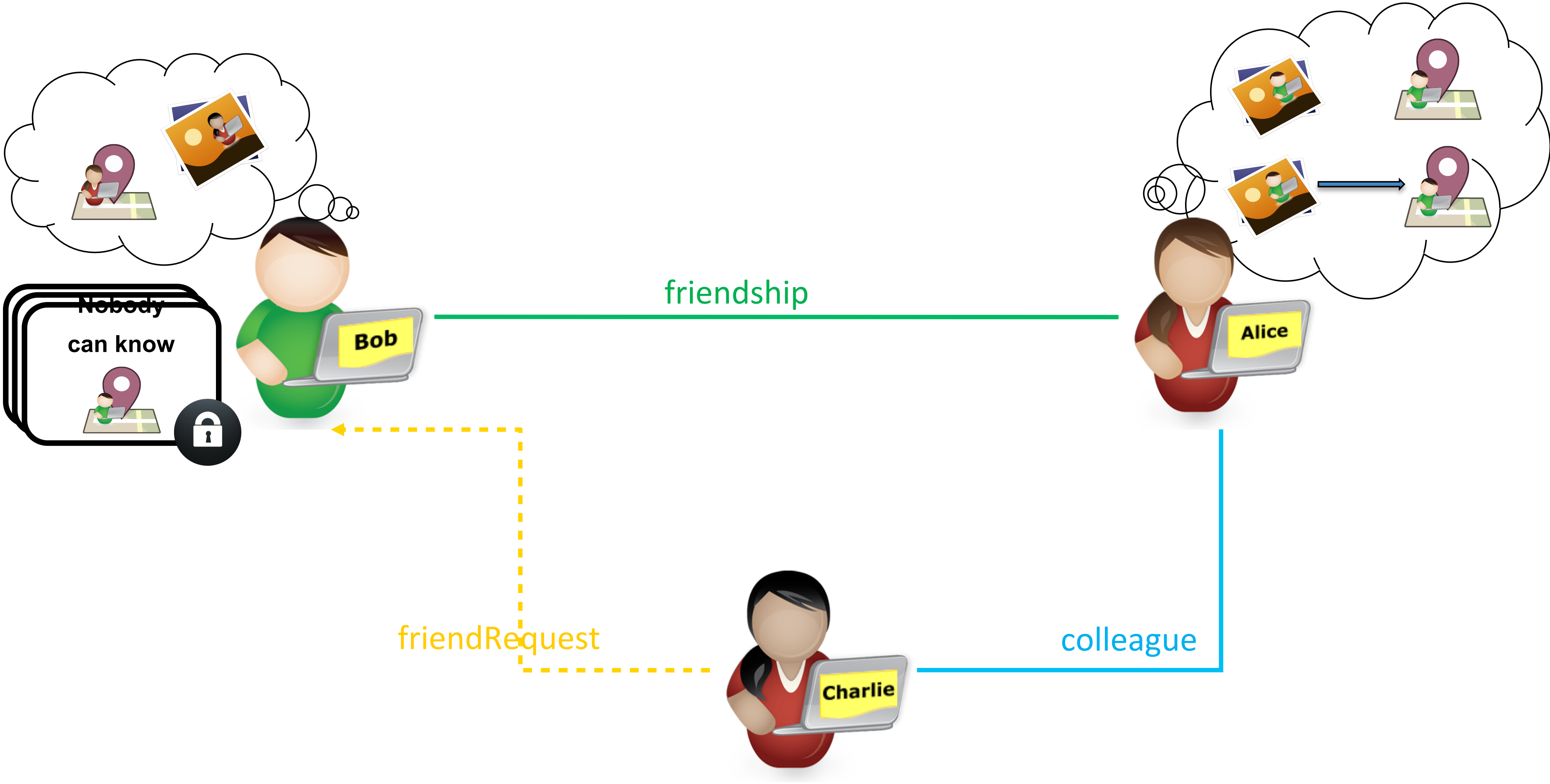
SOCIAL NETWORK GRAPH



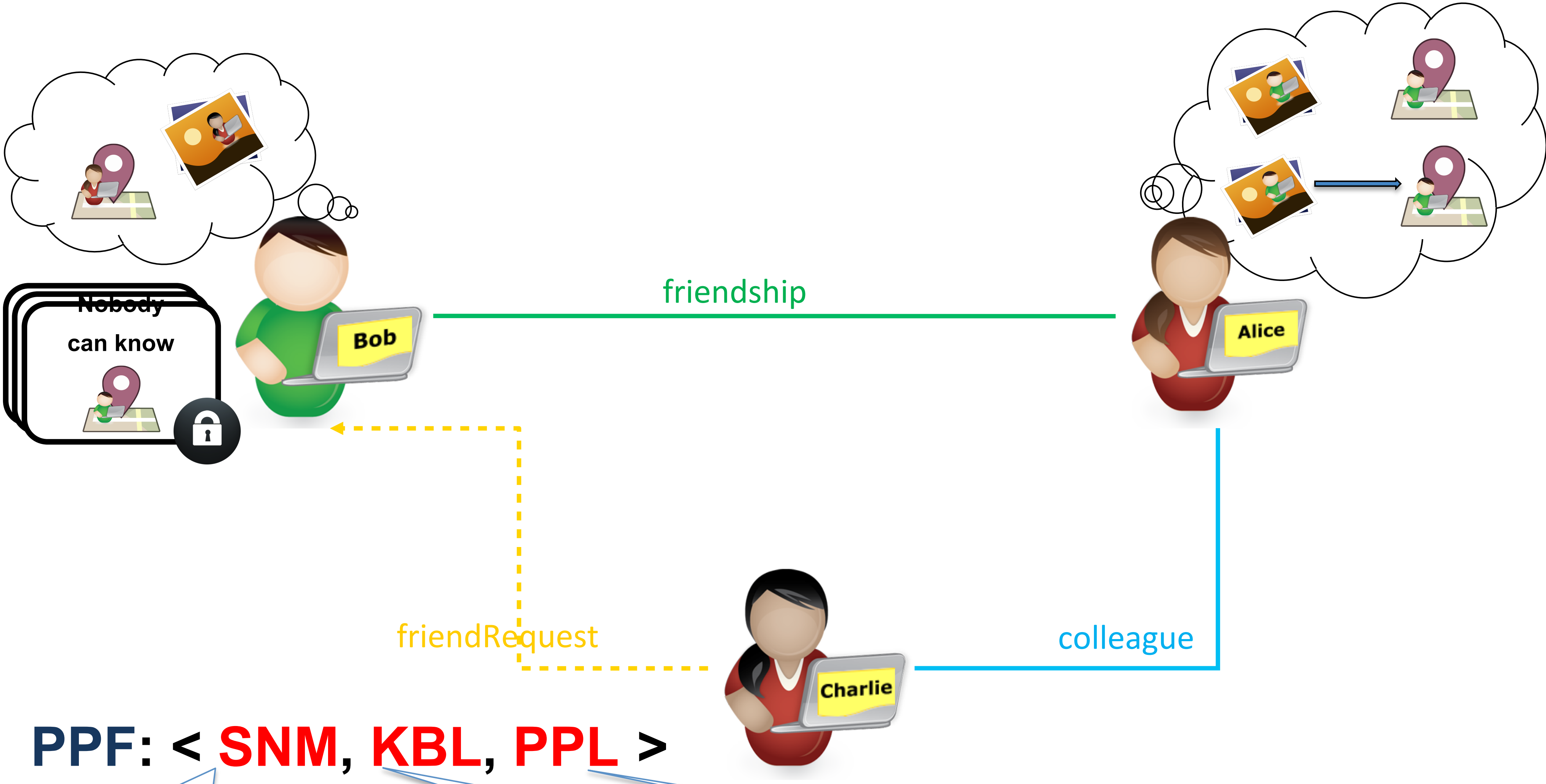
HOW IS IMPLEMENTED? ReBAC



SOCIAL NETWORK GRAPH - REVISITED



PPF: A FORMAL FRAMEWORK FOR PRIVACY POLICIES ON SOCIAL NETWORKS

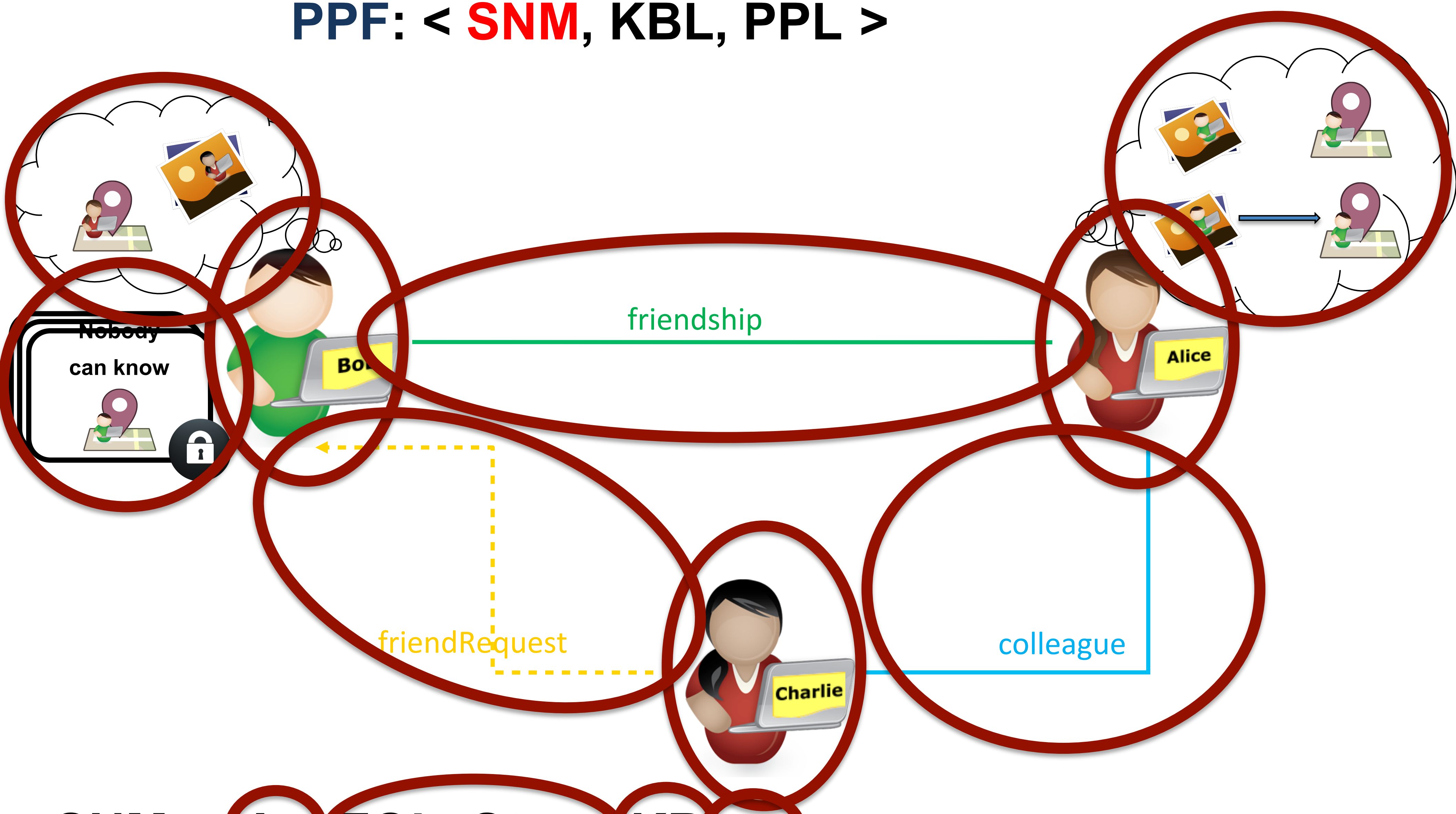


PPF: < SNM, KBL, PPL >

A Social Network Model | **A Knowledge-Based Logic** | **A Privacy Policy Language**

SNM: SOCIAL NETWORK MODELS

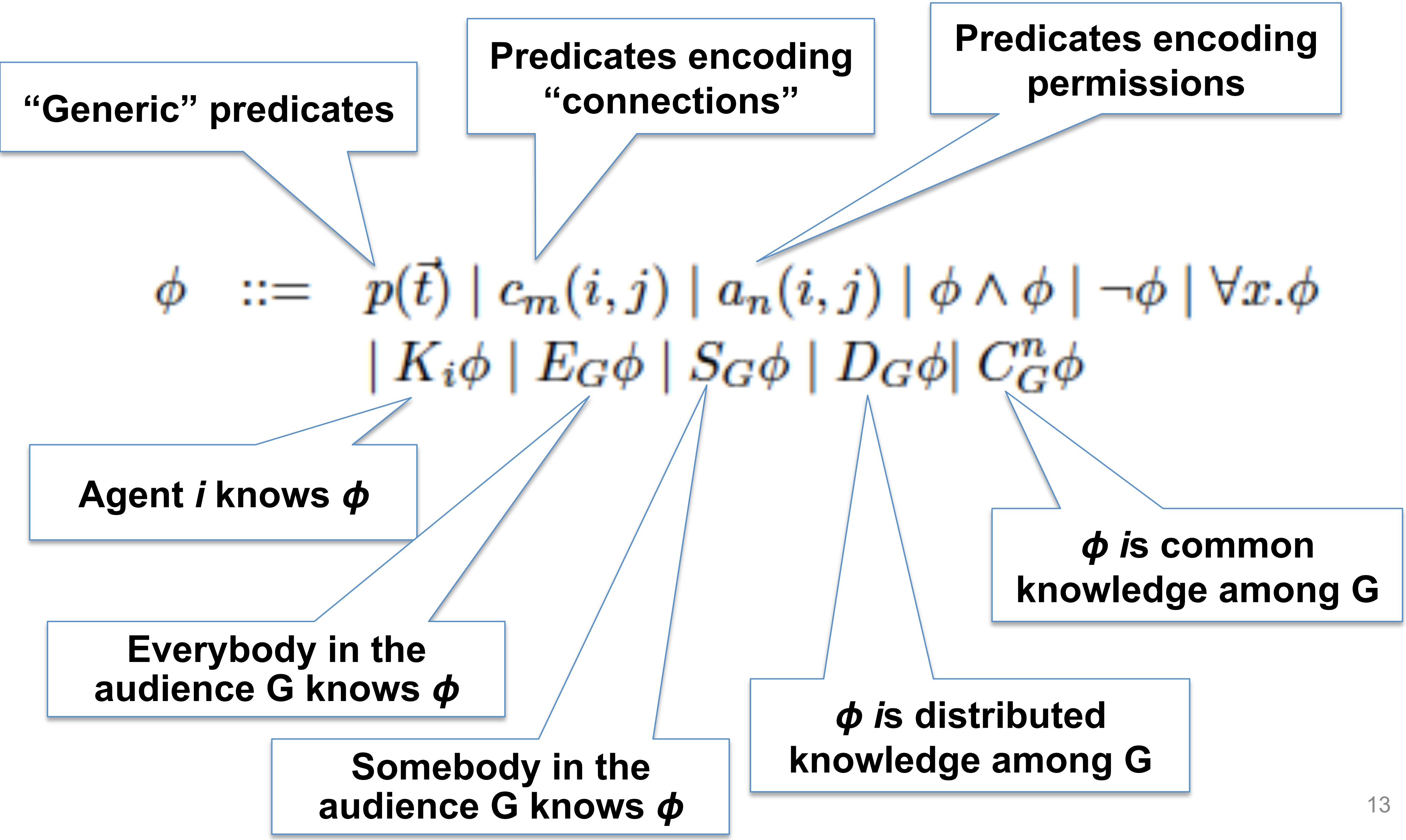
PPF: < SNM, KBL, PPL >



SNM: < Ag, FOL_Struc, KB, π >

KBL: AN “EPISTEMIC” LOGIC

PPF: < SNM, KBL, PPL >



$$\phi ::= p(\vec{t}) \mid c_m(i,j) \mid a_n(i,j) \mid \phi \wedge \phi \mid \neg\phi \mid \forall x.\phi$$
$$\mid K_i\phi \mid E_G\phi \mid S_G\phi \mid D_G\phi \mid C^n_G\phi$$

“Generic” predicates

Predicates encoding “connections”

Predicates encoding permissions

Agent *i* knows *ϕ*

Everybody in the audience G knows *ϕ*

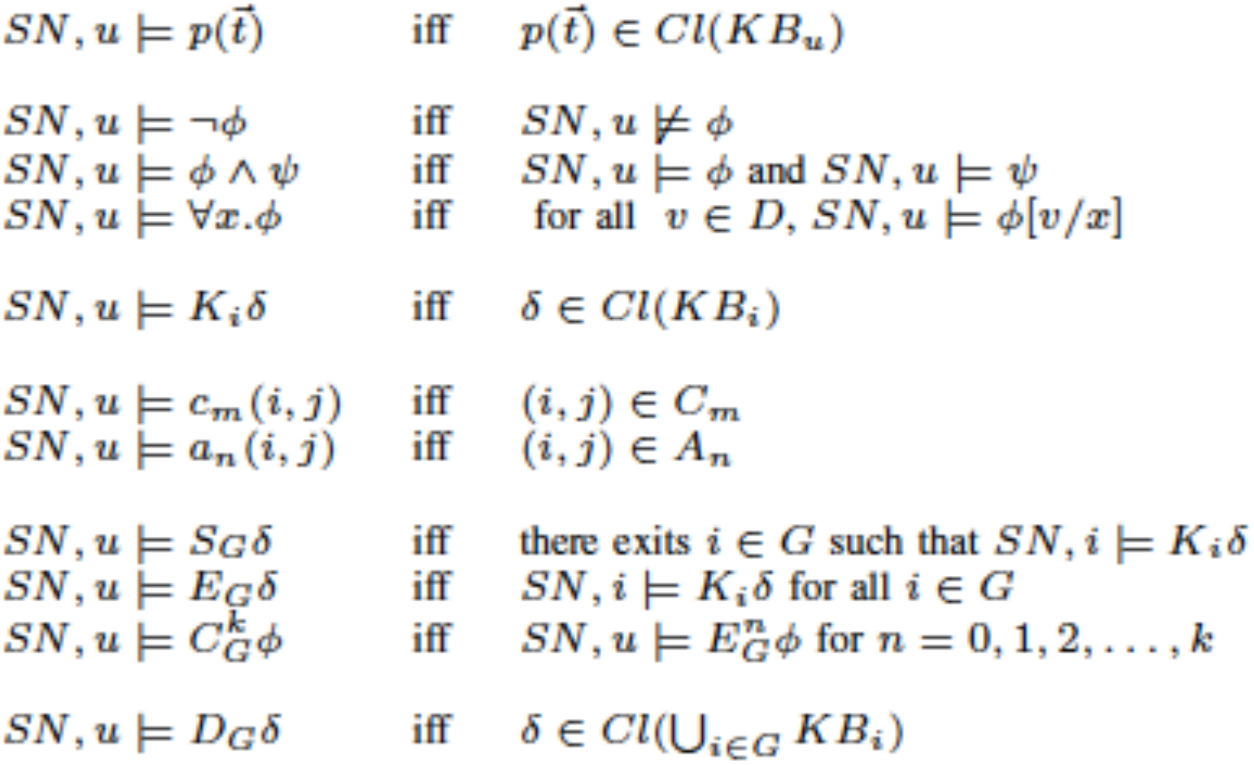
Somebody in the audience G knows *ϕ*

***ϕ is* distributed knowledge among G**

***ϕ is* common knowledge among G**

KBL SEMANTICS

PPF: < SNM, KBL, PPL >



$SN, u \models p(\vec{t})$	iff	$p(\vec{t}) \in Cl(KB_u)$
$SN, u \models \neg\phi$	iff	$SN, u \not\models \phi$
$SN, u \models \phi \wedge \psi$	iff	$SN, u \models \phi$ and $SN, u \models \psi$
$SN, u \models \forall x.\phi$	iff	for all $v \in D$, $SN, u \models \phi[v/x]$
$SN, u \models K_i\delta$	iff	$\delta \in Cl(KB_i)$
$SN, u \models c_m(i, j)$	iff	$(i, j) \in C_m$
$SN, u \models a_n(i, j)$	iff	$(i, j) \in A_n$
$SN, u \models S_G\delta$	iff	there exits $i \in G$ such that $SN, i \models K_i\delta$
$SN, u \models E_G\delta$	iff	$SN, i \models K_i\delta$ for all $i \in G$
$SN, u \models C_G^k\phi$	iff	$SN, u \models E_G^n\phi$ for $n = 0, 1, 2, \ldots, k$
$SN, u \models D_G\delta$	iff	$\delta \in Cl(\bigcup_{i \in G} KB_i)$

TABLE I: $\mathcal{KBL}_{SN}$ satisfiability relation

PPL: SPECIFYING POLICIES

PPF: < SNM, KBL, PPL >

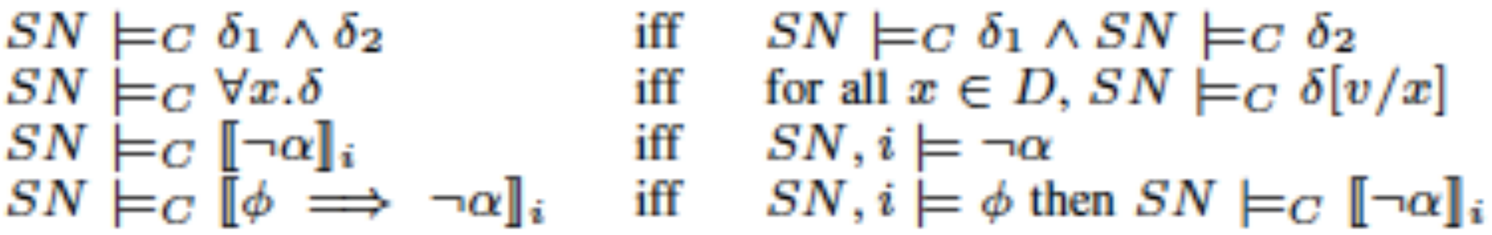
Any KBL formula

Policies of agent *i* (defined over a subset of KBL)

$$
\begin{array}{rcl}
\delta & ::= & \delta \wedge \delta \mid \forall x.\delta \mid [\![\phi \implies \neg\alpha]\!]_i \mid [\![\neg\alpha]\!]_i \\
\alpha & ::= & \alpha \wedge \alpha \mid \psi \mid \gamma' \mid \forall x.\alpha \\
\gamma' & ::= & K_i\gamma \mid E_G\gamma \mid S_G\gamma \mid D_G\gamma \mid C_G^k\gamma \\
\gamma & ::= & \gamma \wedge \gamma \mid \neg\gamma \mid p(\vec{t}) \mid \gamma' \mid \psi \mid \forall x.\gamma \\
\psi & ::= & c_m(i,j) \mid a_n(i,j)
\end{array}
$$

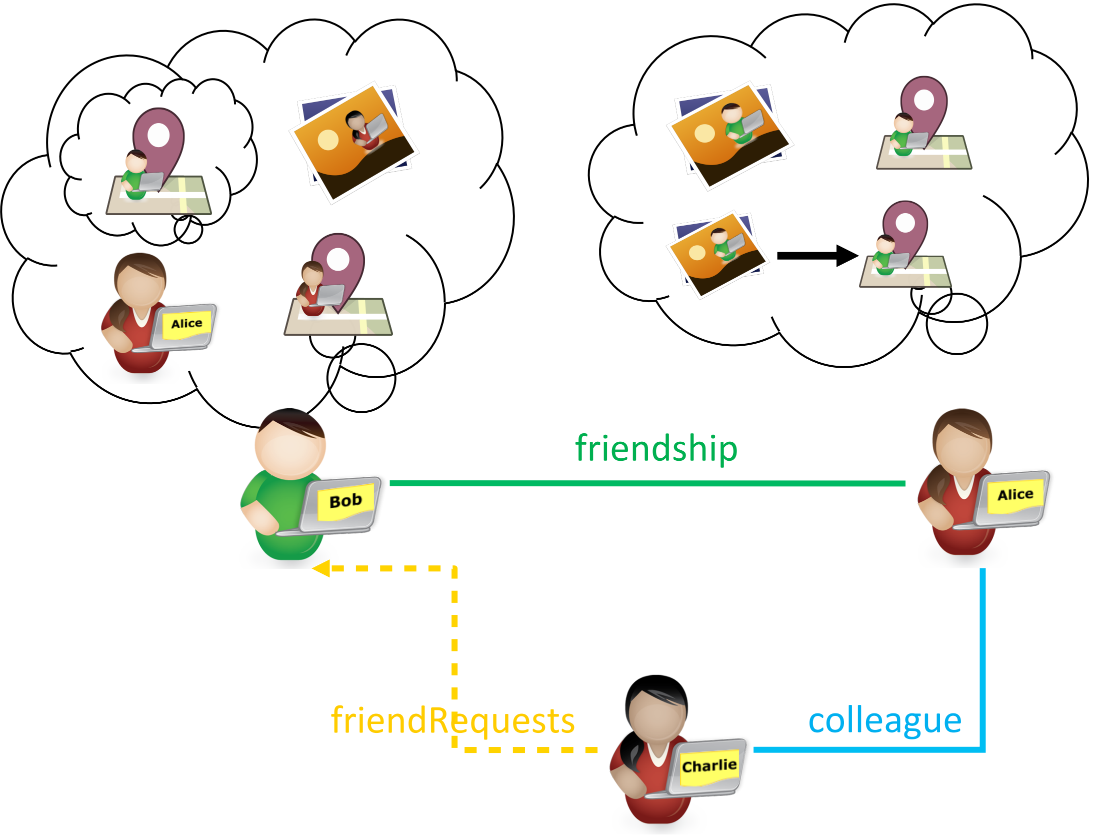
PPL CONFORMANCE RELATION

PPF: < SNM, KBL, PPL >



$$
\begin{array}{lll}
SN \models_C \delta_1 \wedge \delta_2 & \text{iff} & SN \models_C \delta_1 \wedge SN \models_C \delta_2 \\
SN \models_C \forall x.\delta & \text{iff} & \text{for all } x \in D,\ SN \models_C \delta[v/x] \\
SN \models_C [\![\neg\alpha]\!]_i & \text{iff} & SN, i \models \neg\alpha \\
SN \models_C [\![\phi \implies \neg\alpha]\!]_i & \text{iff} & SN, i \models \phi \text{ then } SN \models_C [\![\neg\alpha]\!]_i
\end{array}
$$

KBL - EXAMPLES



- Bob knows Alice's location

K_{Bob} 📍

- Bob knows that Alice knows his location

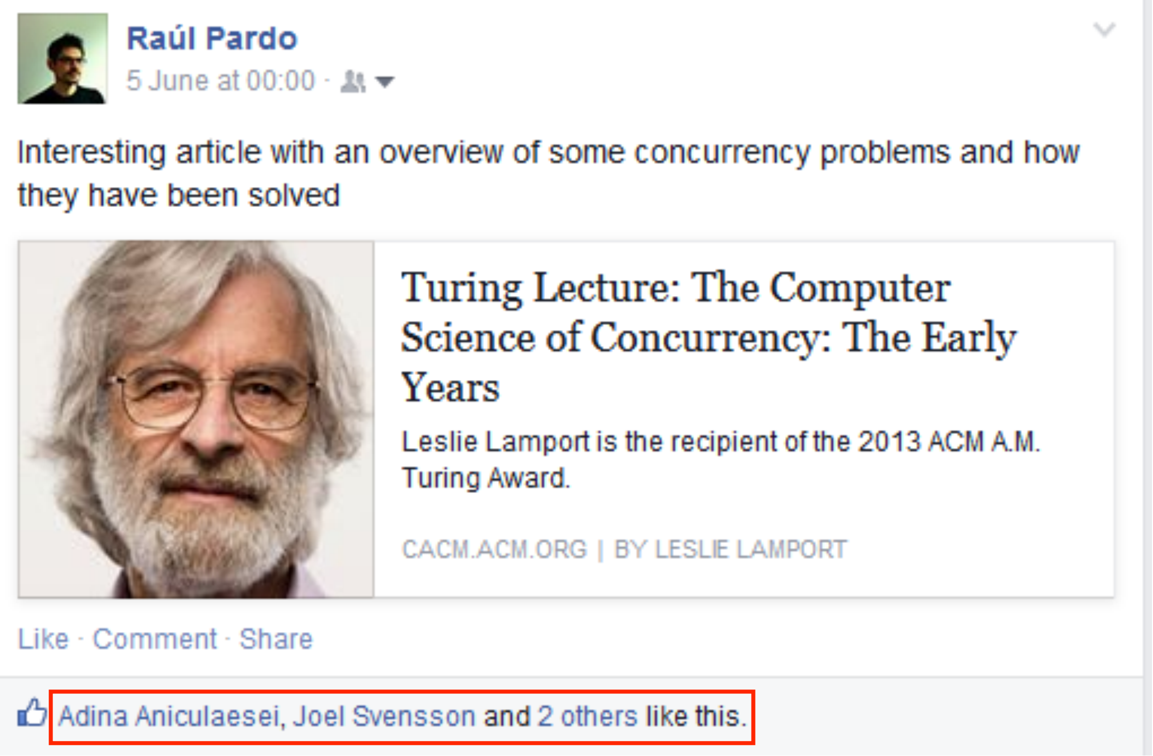
$K_{Bob}\ K_{Alice}$ 📍

- Alice and Bob know Bob's location

$E_{\{Bob,\ Alice\}}$ 📍

KBL - EXAMPLES

- If an agent knows a post, she knows who liked it



Raúl Pardo

5 June at 00:00 ·

Interesting article with an overview of some concurrency problems and how they have been solved

Turing Lecture: The Computer Science of Concurrency: The Early Years

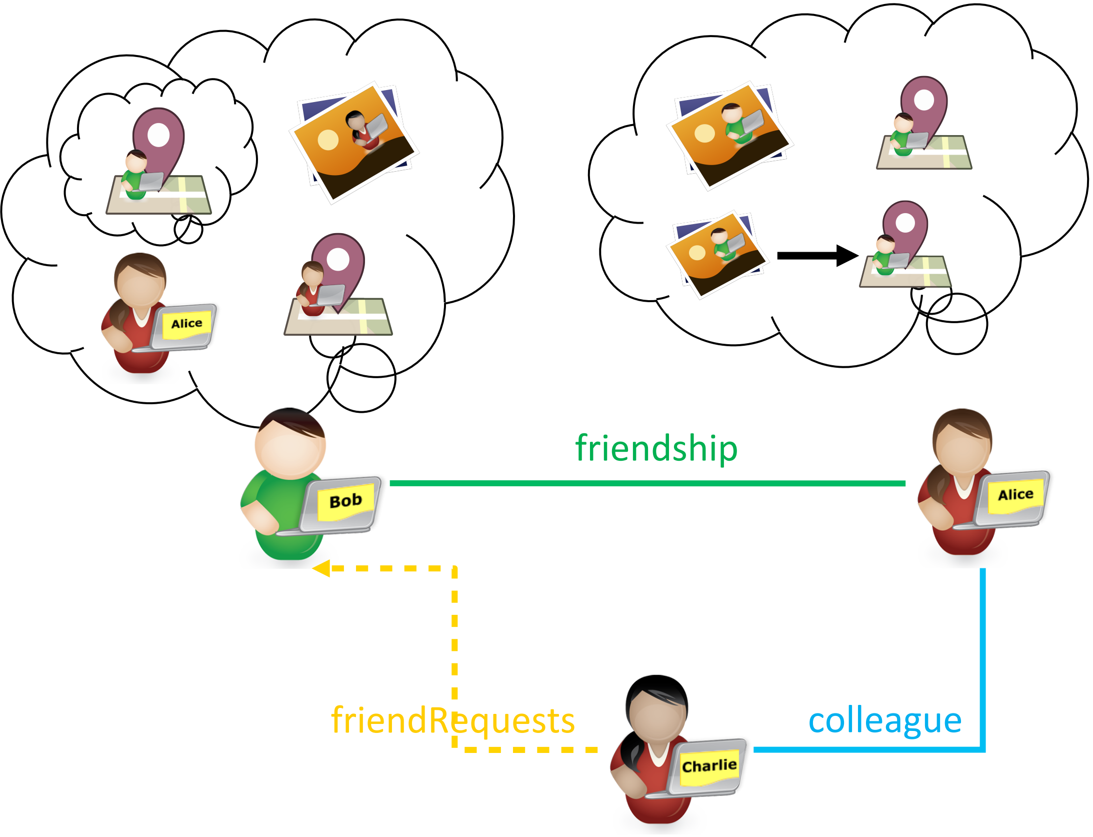
Leslie Lamport is the recipient of the 2013 ACM A.M. Turing Award.

CACM.ACM.ORG | BY LESLIE LAMPORT

Adina Aniculaesei, Joel Svensson and 2 others like this.

$$\forall\, x.\forall\, u.\forall\, i.\forall\, \eta(K_x post(\eta,u)\wedge K_i like(i,u,\eta)\Rightarrow K_x like(i,u,\eta))$$

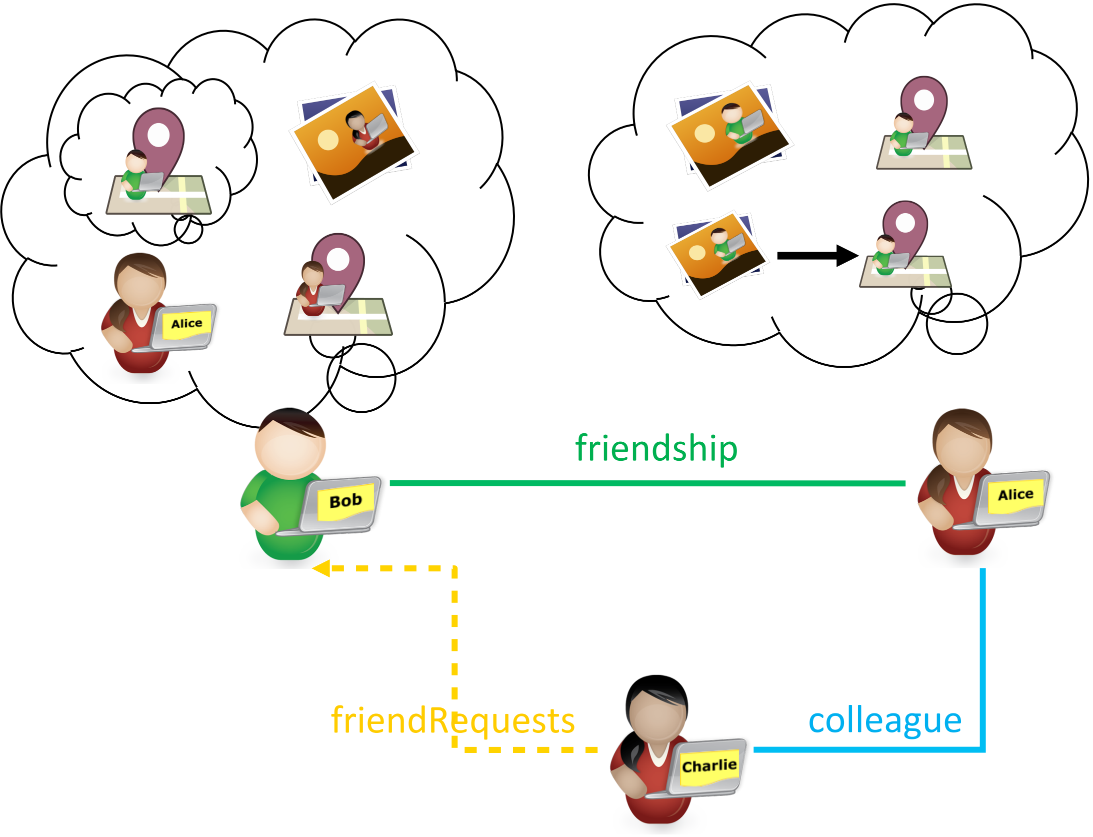
PPL – EXAMPLES



Nobody can know Bob's location (except Bob)

$[\![\neg \, S_{Ag \setminus \{Bob\}}$ $]\!]_{Bob}$

PPL – EXAMPLES



Nobody can know Bob's location (except Bob)

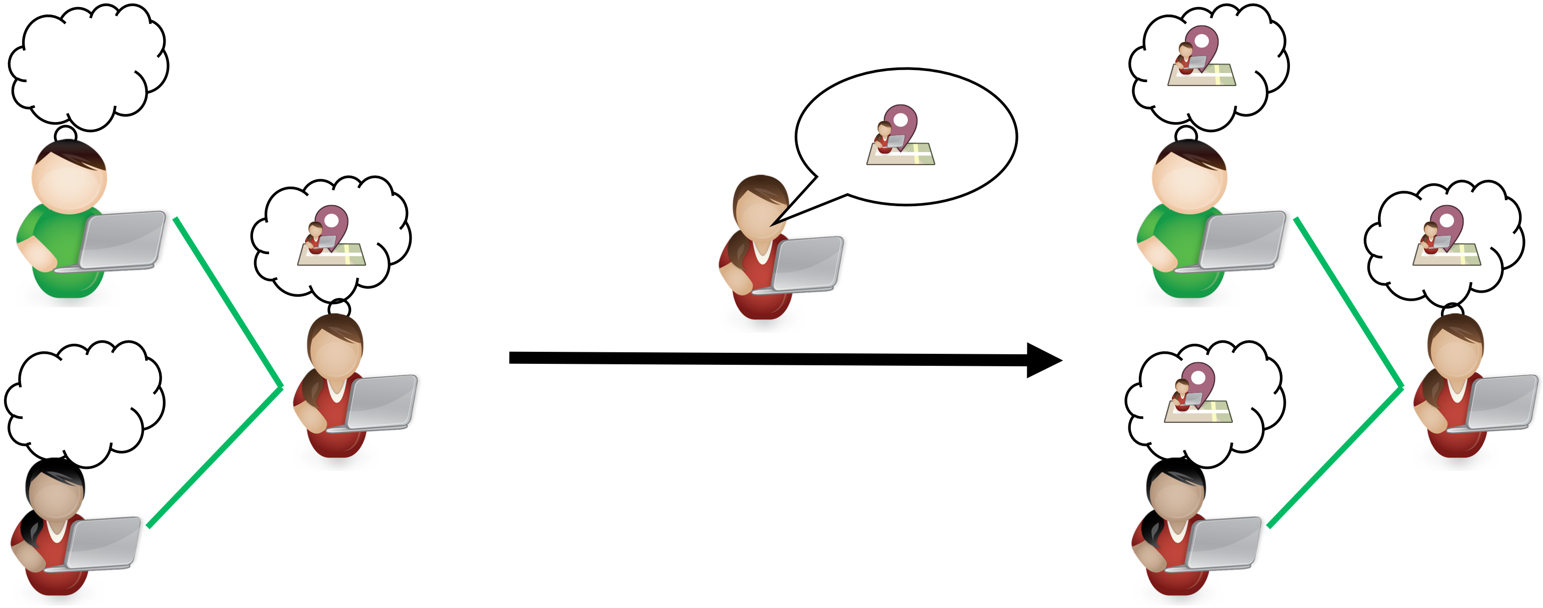
$[\![\neg S_{Ag \setminus \{Bob\}}$ $]\!]_{Bob}$

Only people who liked at least one of Bob's posts can join his event:

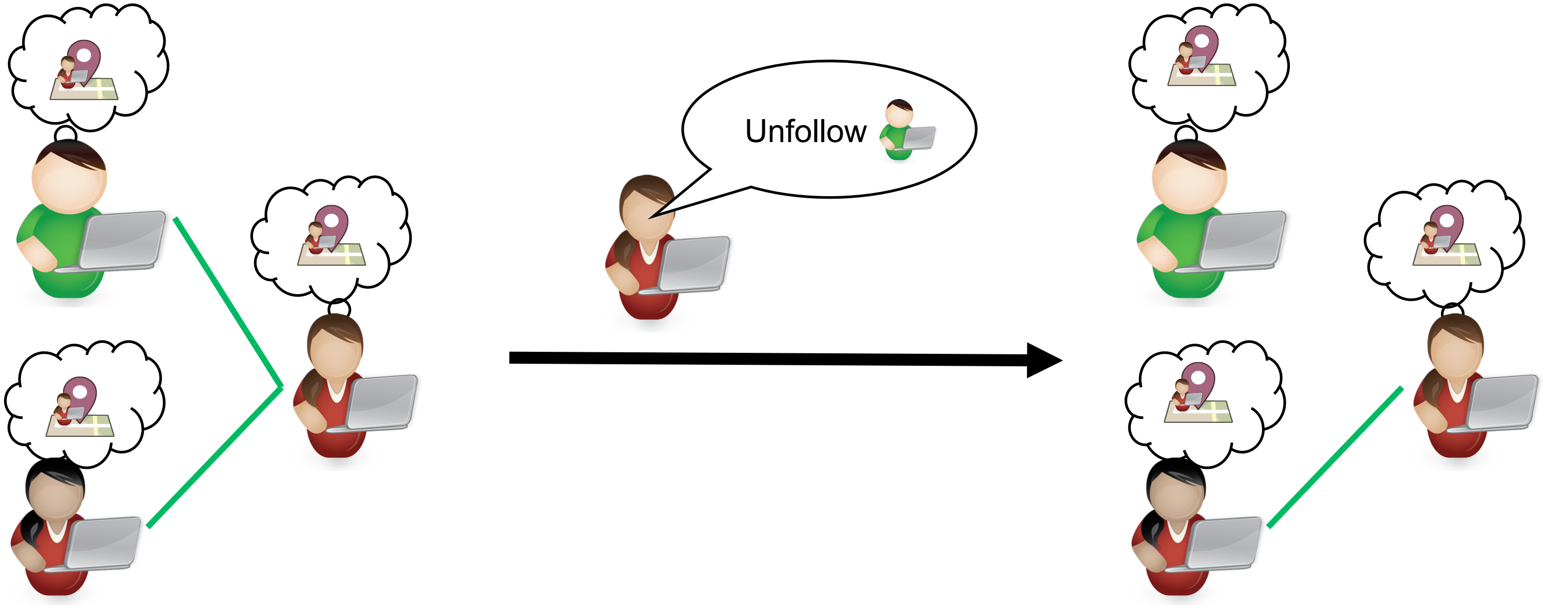
$$\forall i.\forall \eta.[\neg K_{Bob}\, like(i,Bob,\eta) \Rightarrow \neg P_i^{Bob}\, joinEvent]_{Bob}$$

THAT'S NICE BUT…
SOCIAL NETWORKS EVOLVE

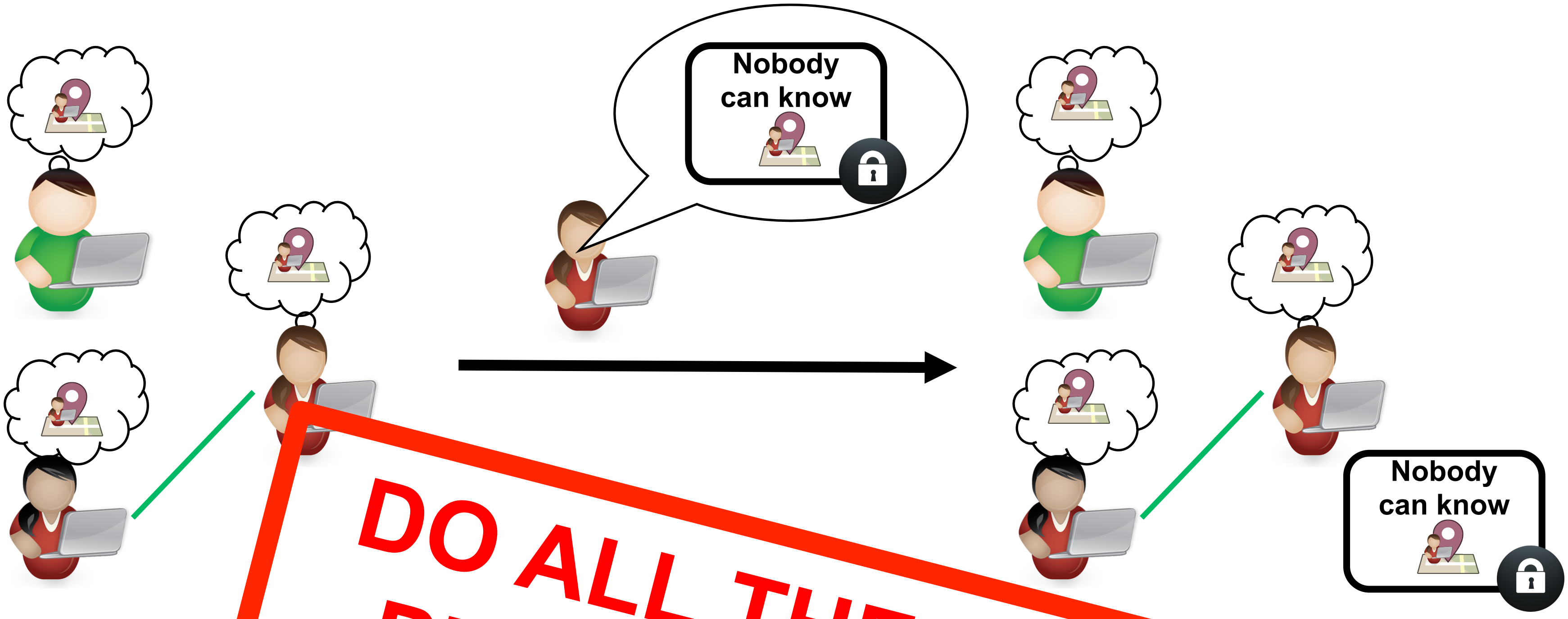
“EPISTEMIC” EVOLUTION



“TOPOLOGICAL” EVOLUTION

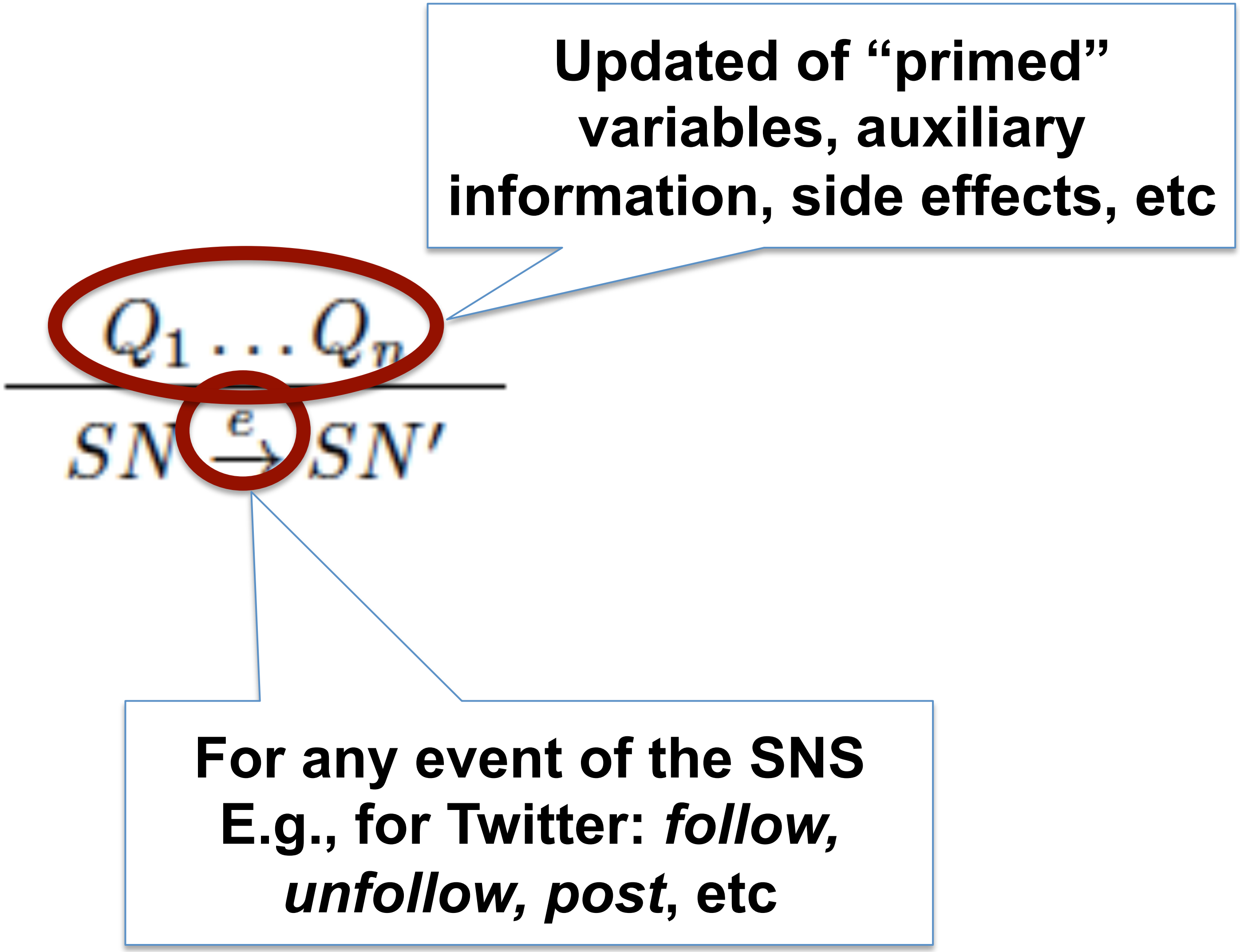


“POLICY” EVOLUTION



DO ALL THESE EVENTS PRESERVE PRIVACY?

OPERATIONAL RULES

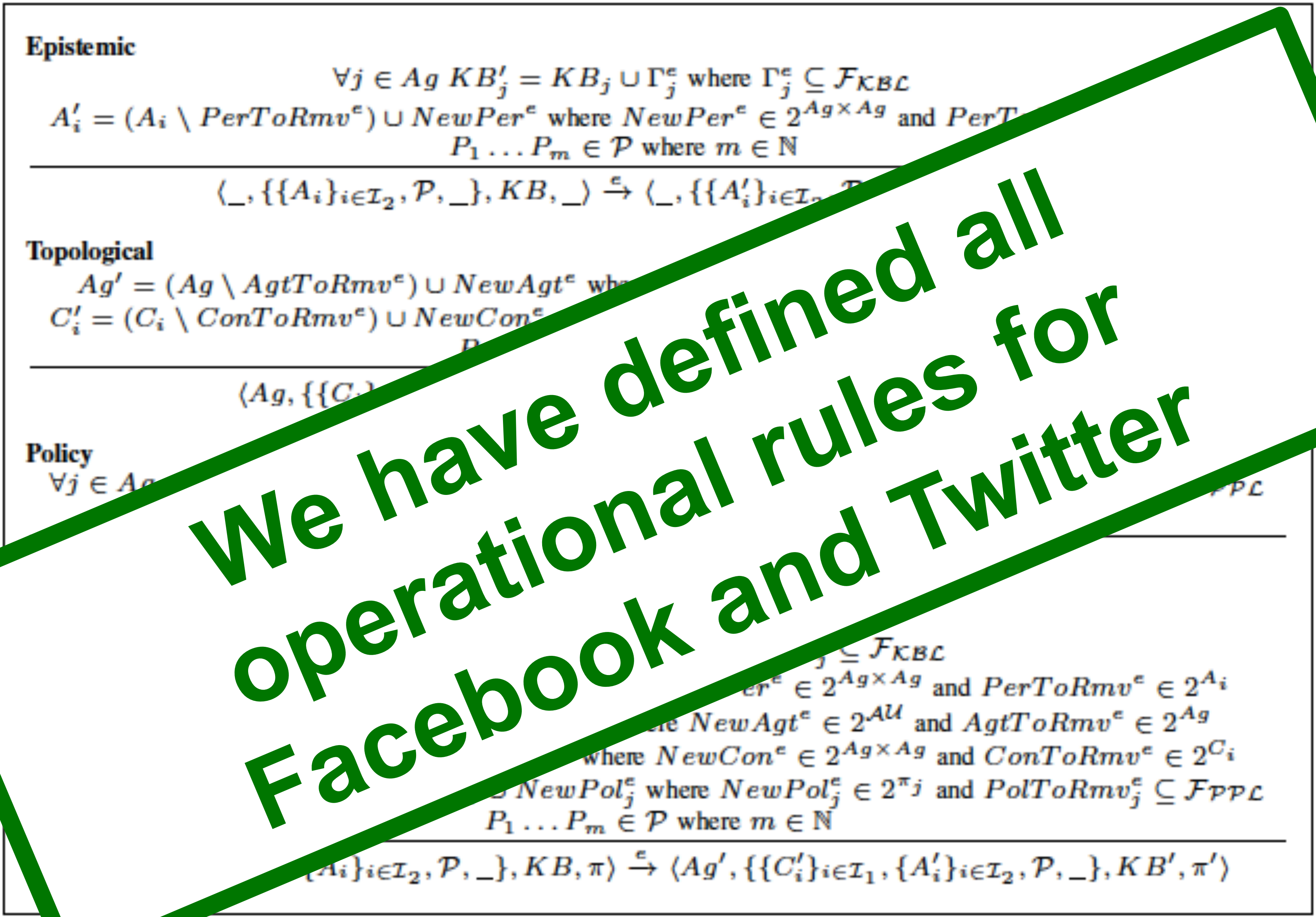


Updated of “primed” variables, auxiliary information, side effects, etc

$$\frac{Q_1 \ldots Q_n}{SN \xrightarrow{e} SN'}$$

For any event of the SNS E.g., for Twitter: *follow, unfollow, post*, etc

OPERATIONAL RULES: GENERIC STRUCTURE



Epistemic

$$\forall j \in Ag\ KB'_j = KB_j \cup \Gamma^e_j \text{ where } \Gamma^e_j \subseteq \mathcal{F}_{\mathcal{KBL}}$$

$$A'_i = (A_i \setminus PerToRmv^e) \cup NewPer^e \text{ where } NewPer^e \in 2^{Ag \times Ag} \text{ and } PerT$$

$$P_1 \ldots P_m \in \mathcal{P} \text{ where } m \in \mathbb{N}$$

$$\langle \_, \{\{A_i\}_{i \in \mathcal{I}_2}, \mathcal{P}, \_\}, KB, \_\rangle \xrightarrow{e} \langle \_, \{\{A'_i\}_{i \in \mathcal{I}_2}, \mathcal{P}$$

Topological

$$Ag' = (Ag \setminus AgtToRmv^e) \cup NewAgt^e \text{ wh}$$

$$C'_i = (C_i \setminus ConToRmv^e) \cup NewCon^e$$

$$\langle Ag, \{\{C_i\}$$

Policy

$$\forall j \in Ag$$

$$\mathcal{F}_{\mathcal{PPL}}$$

$$\subseteq \mathcal{F}_{\mathcal{KBL}}$$

$$er^e \in 2^{Ag \times Ag} \text{ and } PerToRmv^e \in 2^{A_i}$$

$$NewAgt^e \in 2^{\mathcal{AU}} \text{ and } AgtToRmv^e \in 2^{Ag}$$

$$\text{where } NewCon^e \in 2^{Ag \times Ag} \text{ and } ConToRmv^e \in 2^{C_i}$$

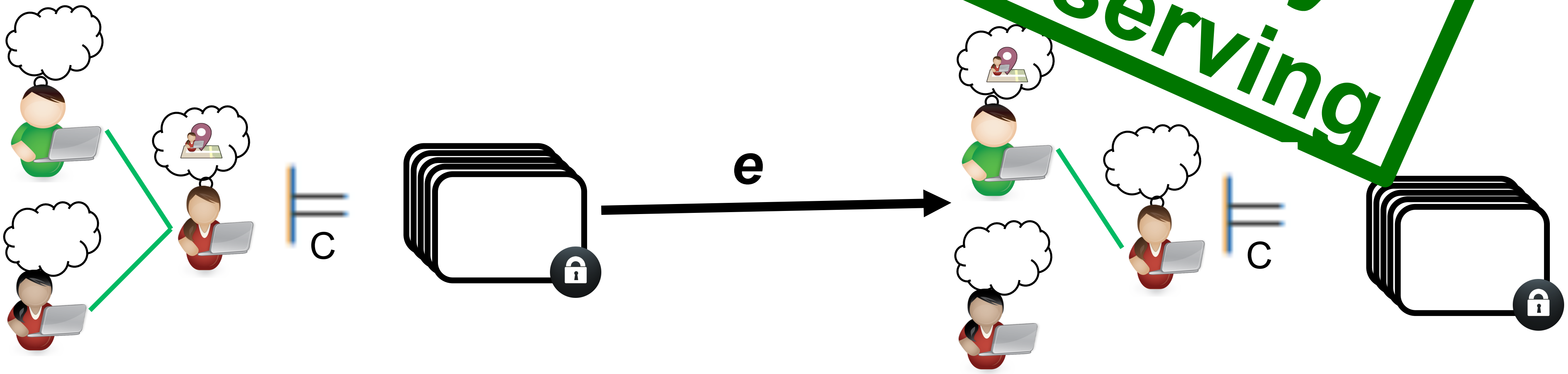
$$\cup NewPol^e_j \text{ where } NewPol^e_j \in 2^{\pi_j} \text{ and } PolToRmv^e_j \subseteq \mathcal{F}_{\mathcal{PPL}}$$

$$P_1 \ldots P_m \in \mathcal{P} \text{ where } m \in \mathbb{N}$$

$$\{A_i\}_{i \in \mathcal{I}_2}, \mathcal{P}, \_\}, KB, \pi\rangle \xrightarrow{e} \langle Ag', \{\{C'_i\}_{i \in \mathcal{I}_1}, \{A'_i\}_{i \in \mathcal{I}_2}, \mathcal{P}, \_\}, KB', \pi'\rangle$$

We have defined all operational rules for Facebook and Twitter

PRESERVATION OF PRIVACY



Privacy Preserving

THEOREM: 🐦 **and** f **are privacy preserving**

SUMMARY

- Formal Privacy Policy Framework (SEFM’14)
  - Social Network Model – SN
  - Knowledge Based Logic – KBL
  - Privacy Policy Language – PPL
  - Formalization of Facebook and Twitter

- Evolution of SNs (under submission)
  - Operational rules
  - Privacy preservation
  - Applied to Facebook and Twitter

ON-GOING AND FUTURE WORK

- Proving relation of the SN Model with standard Kripke semantics for Epistemic Logic
- Implementation: Diaspora*

- Extending the framework with real-time
- Attacker model
- Enforcement mechanisms

Long Term:

- A generic privacy policy framework controlling your device (e.g., smart phone)
- Privacy-preserving contractual agreements

Part II

Other (current) research interests

SPECIFICATION AND ANALYSIS OF NORMATIVE TEXTS

Joint work with

John C. Camilleri

Also:

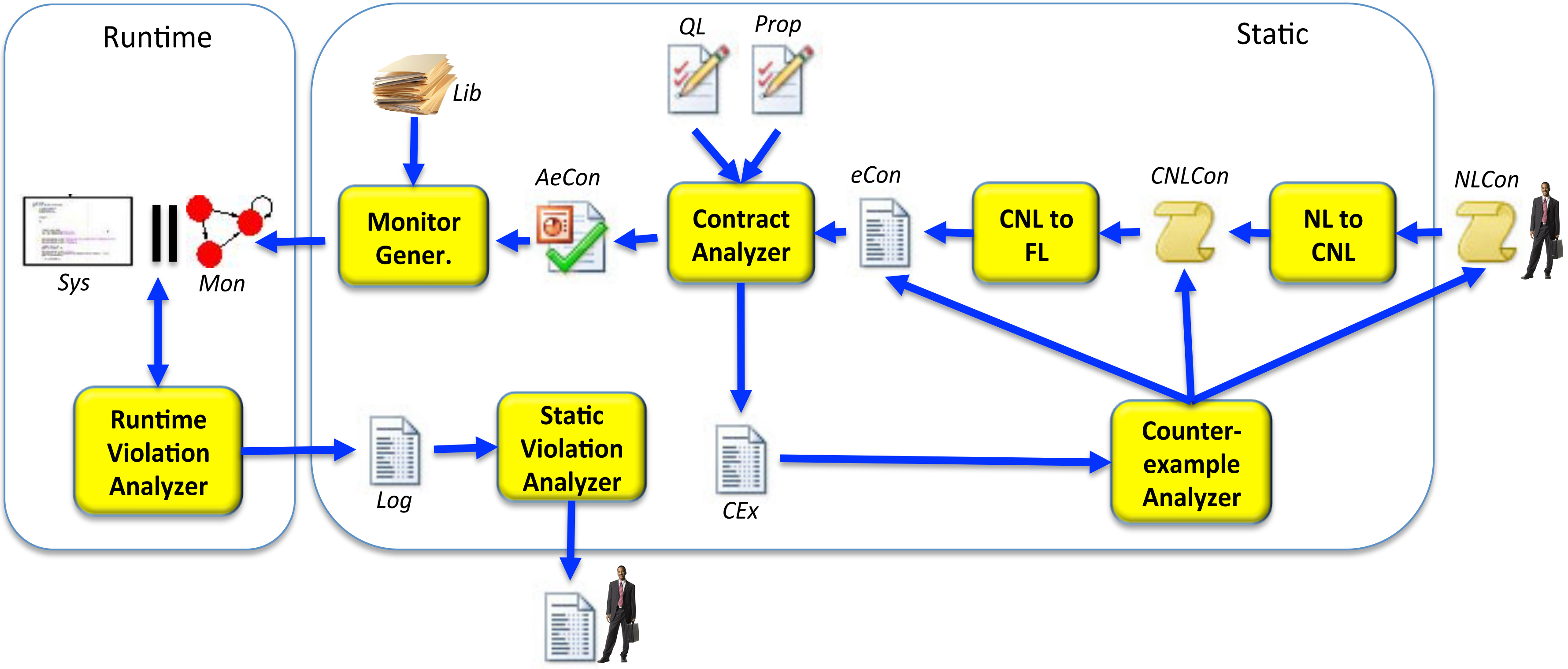
Cristian Prisacariu, Gordon Pace, …

WHAT DO WE WANT TO DO?

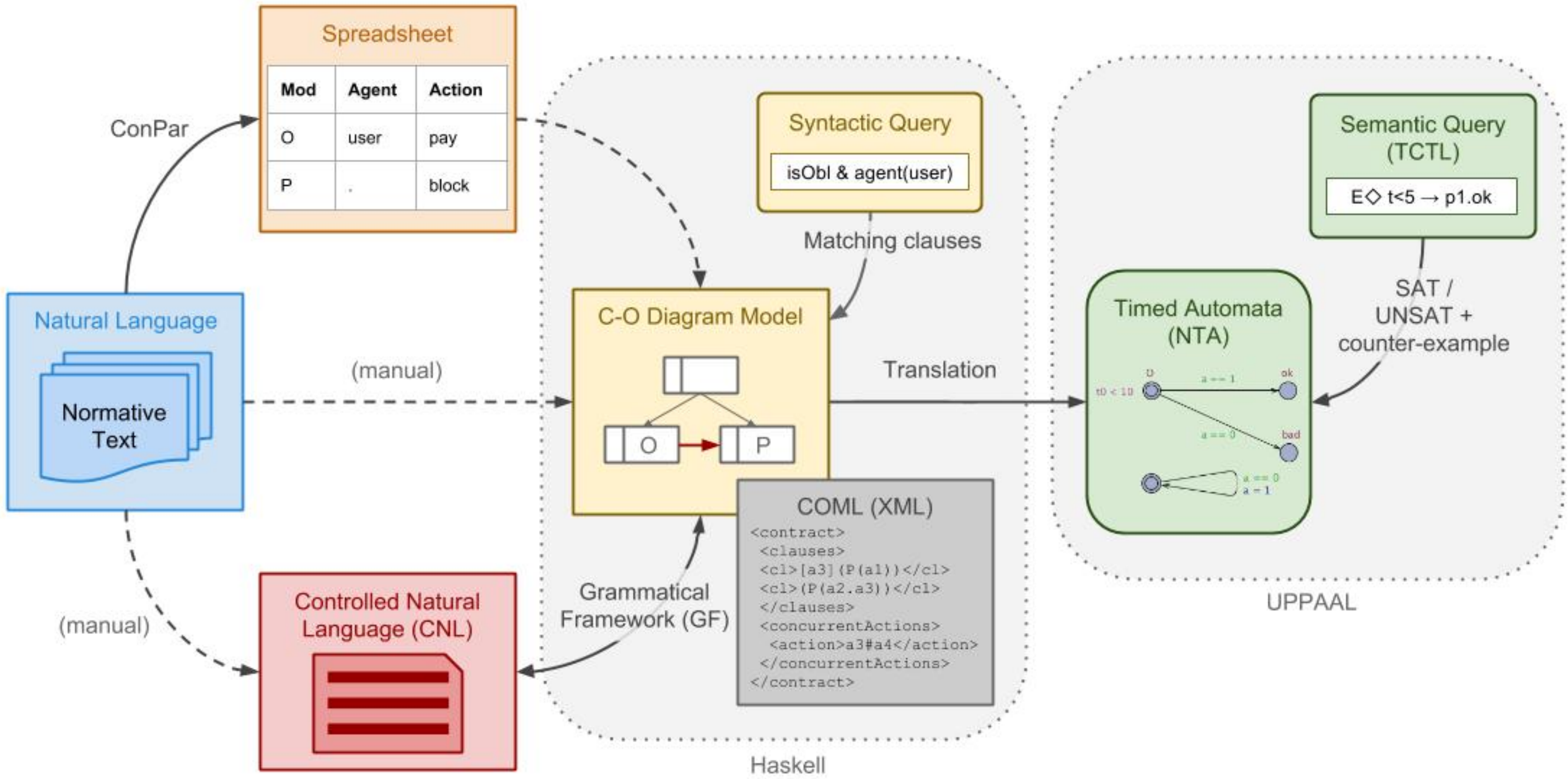
- **Formalize** ”contracts” (normative texts)
- Provide (semi) automatic tools for **analysis**

“What happens if the customer skips the payment?”
“What is the shortest service utilization?”
”What are my obligations?”
”Are there obligations without ”reparations”?

THE BIG (PARTIAL) PICTURE…



STATUS



Mod	Agent	Action
O	user	pay
P	.	block

```
<contract>
 <clauses>
 <cl>[a3](P(a1))</cl>
 <cl>(P(a2.a3))</cl>
 </clauses>
 <concurrentActions>
  <action>a3#a4</action>
 </concurrentActions>
</contract>
```

Our work on “contracts”:

FMOODS'07, ATVA'07, ATVA'08, ATVA'09, iFM'09, FESCA'09, WOLLIC'09, ICAIL'09, ICTAC'09, IEEE SCC'10, FMSPLE'10, FLACOS'11, JLAP'12, JLAP’13, IEEE TSE'14, CNL’14

* Thanks to John Camilleri for the picture

COMBINING STATIC AND RUNTIME VERIFICATION

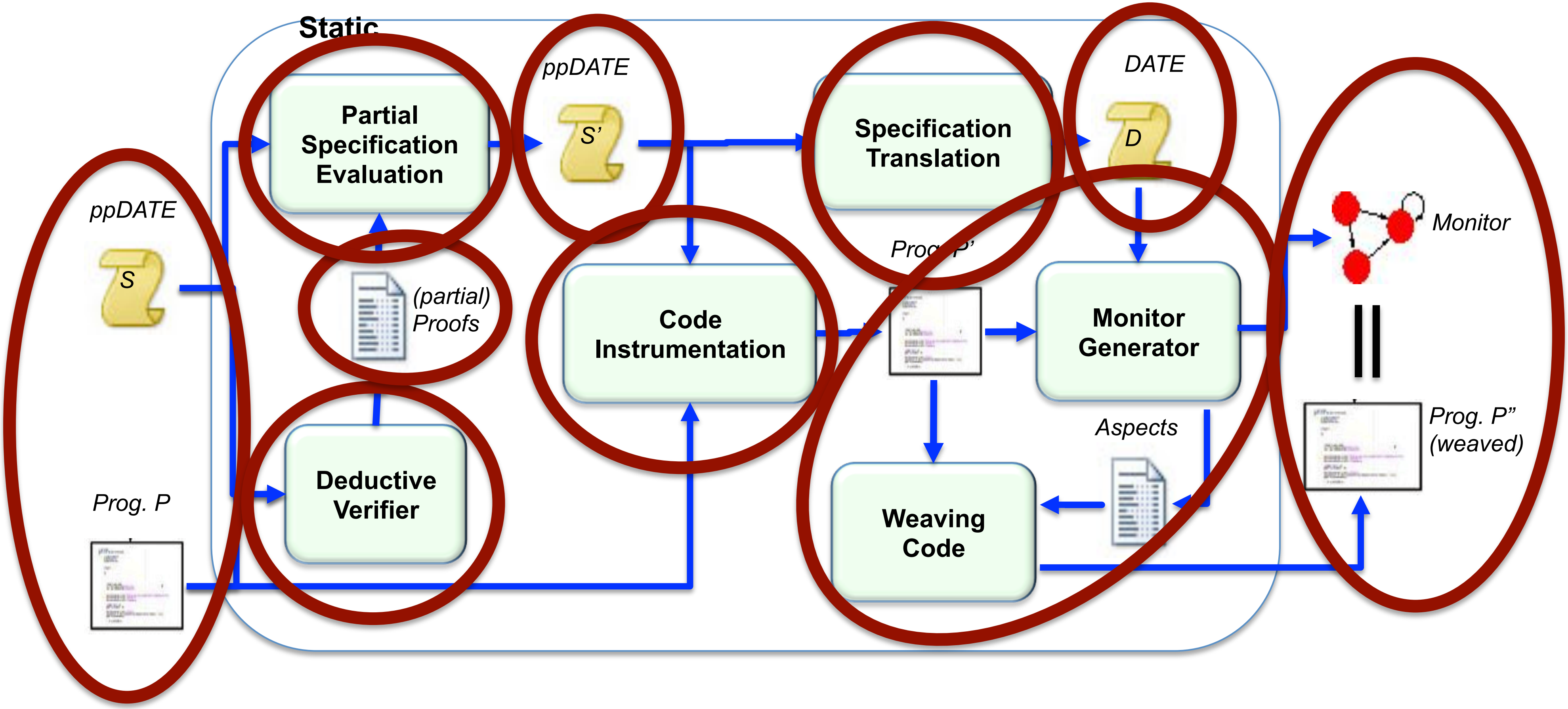
(To verify Data- and Control-Oriented properties)

Joint work with

Wolfgang Ahrendt, Mauricio Chimento and Gordon Pace

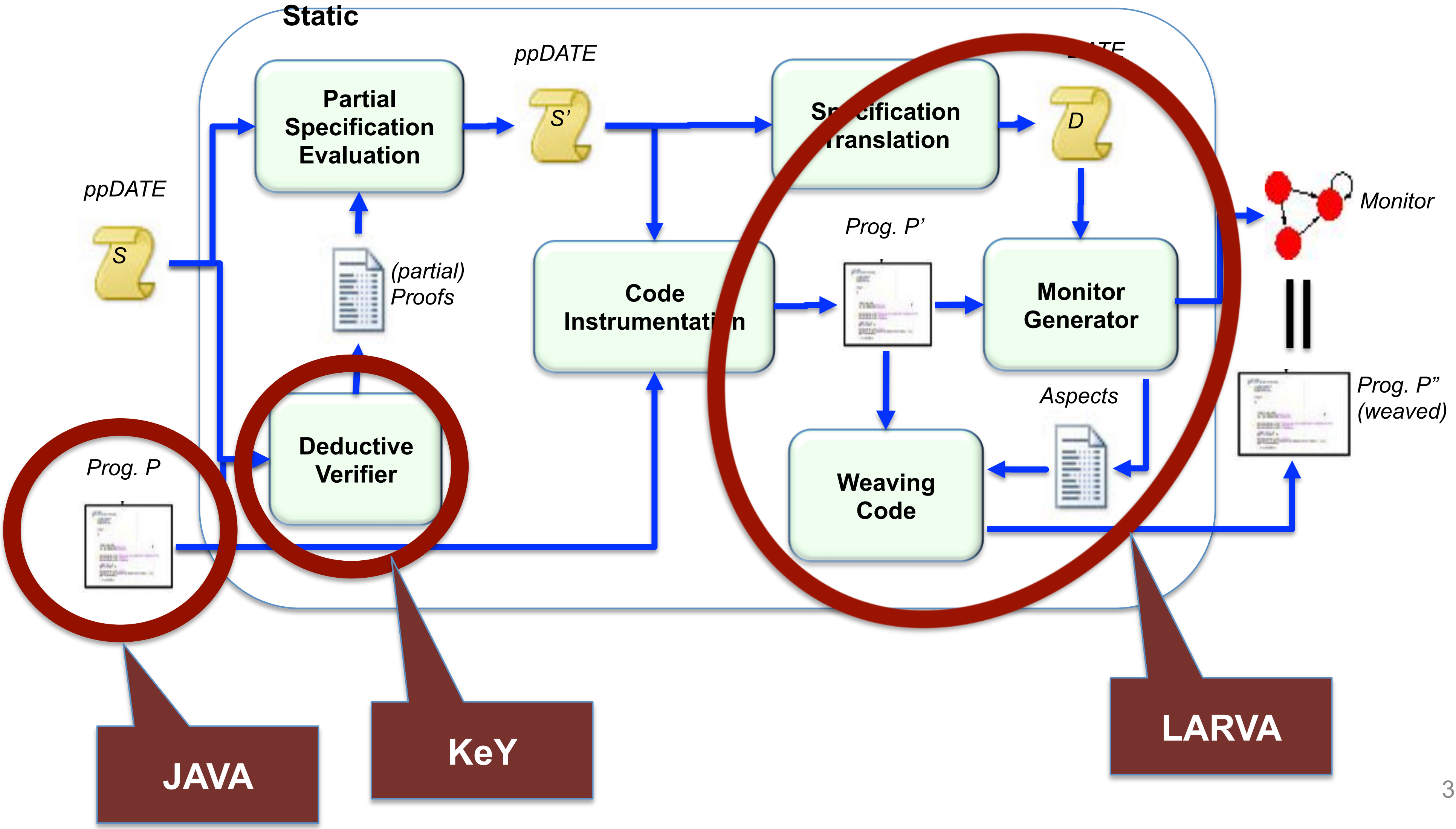
STARVOORS

Unified **Sta**tic and **R**untime **V**erification of **O**bject-**O**riented **S**oftware



STARVOORS

Unified **Stat**ic and **R**untime **V**erification of **O**bject-**Or**iented **S**oftware



Static

ppDATE

S

Partial Specification Evaluation

ppDATE

S'

(partial) Proofs

Specification Translation

DATE

D

Code Instrumentation

Prog. P'

Monitor Generator

Monitor

Prog. P

Deductive Verifier

Aspects

Weaving Code

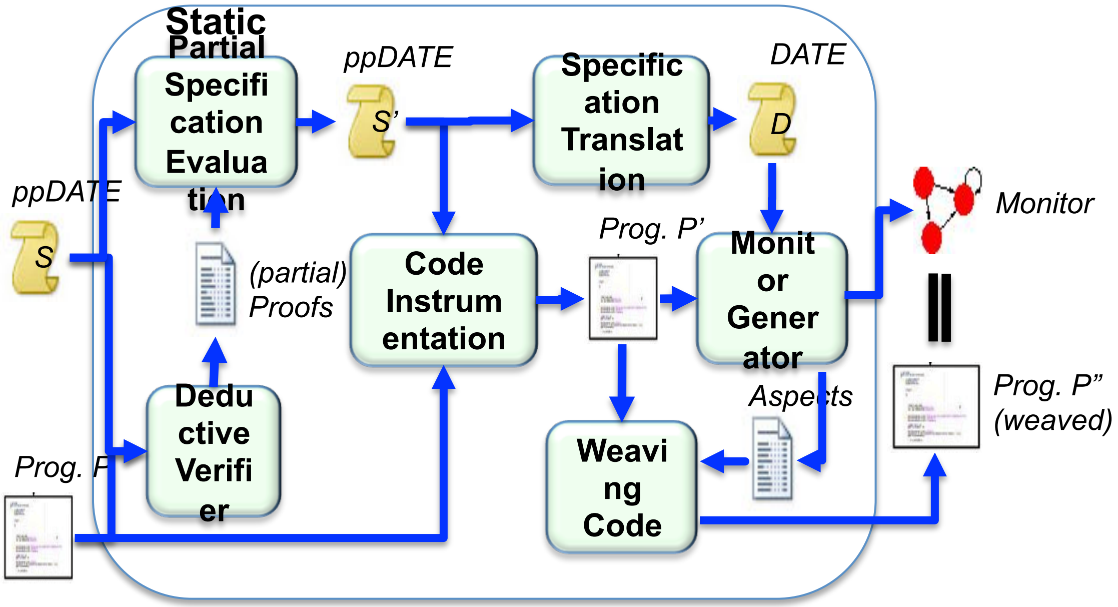
Prog. P" (weaved)

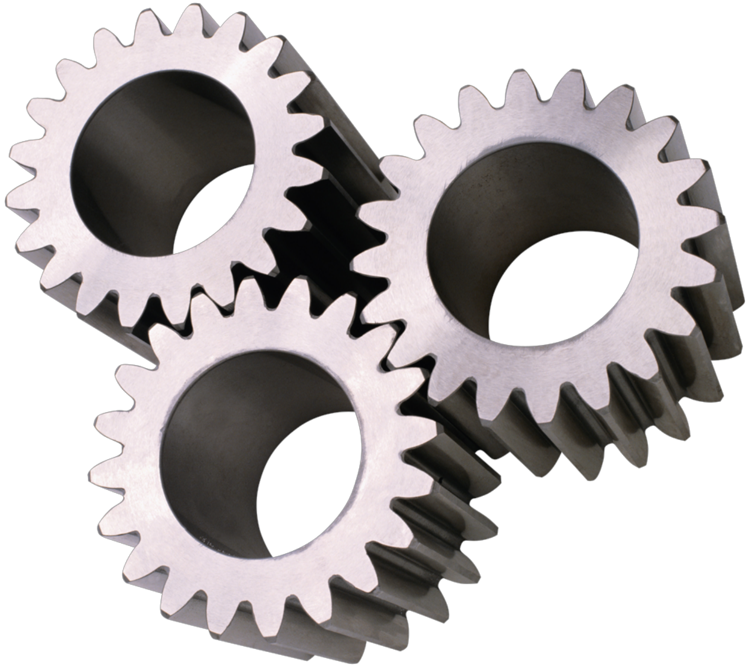
JAVA

KeY

LARVA

STATUS





Framework + ppDATE (FM'15)

Automatic Tool (RV'15)

THANKS