The Regorous Methodology to Business Process Compliance

Guido Governatori
13 December 2017

www.data61.csiro.au
A Privacy Act

Section 1: (Prohibition to collect personal medical information)

**Offence:** It is an offence to collect personal medical information.

**Defence:** It is a defence to the prohibition of collecting personal medical information, if an entity immediately destroys the illegally collected personal medical information before making any use of the personal medical information.

Section 2: An entity is permitted to collect personal medical information if the entity acts under a Court Order authorising the collection of personal medical information.

Section 3: (Prohibition to collect personal information) It is forbidden to collect personal information unless an entity is permitted to collect personal medical information.

**Offence:** an entity collected personal information

**Defence:** an entity being permitted to collect personal medical information.
Making Sense of the Act

- Collection of medical information is forbidden.
- Destruction of the illegally collected medical information excuses the illegal collection.
- Collection of medical information is permitted if there is an authorising court order.
- Collection of personal information is forbidden.
- Collection of personal information is permitted if the collection of medical information is permitted.
Are We Compliant?

The Regorous Methodology to Business Process Compliance | Guido Governatori
Governatori “Thou Shalt is not You Will” showed that temporal logics are not suitable to represent norms (and the result extend to the vast majority of deontic logics).

Governatori and Hashmi “No Time for Compliance” showed that compliance frameworks based on (linear) temporal logic are not able to handle the scenario correctly.
The Regorous Approach

1. Annotated business process models
2. Proper representation of norms based on PCL (Process Compliance Logic)
3. Simulate execution of traces and round trips to PCL reasoner
   1. Determine what are the obligations in force for each state
   2. Determine which obligations have been fulfilled, violated, or pending
   3. Determine which violations have been compensated for

http://www.regorous.com
Modelling Processes

$t_1: A, B, C, D, E, F, H$
$t_2: A, B, D, C, E, F, H$
$t_3: A, D, B, C, E, F, H$

$t_4: A, B, C, D, E, G, H$
$t_5: A, B, D, C, E, G, H$
$t_6: A, D, B, C, E, G, H$
Annotated Traces

Let $\text{Lit}$ be a set of literals, $T$ be the set of traces of a process and $\mathbb{N}$ be the set of natural numbers.

$$\text{State}: T \times \mathbb{N} \mapsto 2^\text{Lit}$$

The function $\text{State}$ returns the set of literals describing “what’s going on in a trace $t$ after the execution of the $n$-th task in the process”.
Example

Tasks
- A: “turn the light on”
- B: “check if glass is empty”
- C: “fill glass with water”
- D: “turn glass upside-down”

Propositions
- p: “the light is on”
- q: “the glass is full”

Trace 1: ⟨A, B, D⟩
Trace 2: ⟨A, B, C, D⟩

- State(i, 1) = \{ p \}, \; i \in \{ 1, 2 \}
- State(1, 2) = \{ p, q \}
- State(2, 2) = \{ p, \neg q \}
- State(2, 3) = \{ p, q \}
- State(1, 3) = \{ p, \neg q \}
- State(2, 4) = \{ p, \neg q \}
Modelling Norms

Norms are modelled as if ... then ... rules

- norms are defeasible (handling exceptions)
- two types of norms
  - constitutive rules: defining terms used in a legal context
    \[ A_1, \ldots, A_n \Rightarrow C \]
  - prescriptive rules: defining “normative effects” (i.e., obligations, permissions, prohibitions ...)
    \[ A_1, \ldots, A_n \Rightarrow [O]C_1 \otimes [O]C_2 \otimes \cdots \otimes [O]C_m \]
    \[ A_1, \ldots, A_n \Rightarrow [P]C \]
1. $A$ is a fact; or

2. there is an applicable rule for $A$, and either
   1. all the rules for $\neg A$ are discarded (i.e., not applicable) or
   2. every applicable rule for $\neg A$ is weaker than an applicable rule for $A$. 

Reasoning with Norms
The Regorous Architecture

Compliance Rule Base
- Rule 1
- Rule 2
- Rule 3
- Rule 4
- Rule 5
- Rule 6
- Rule 7
- Rule 8
- Rule 9
- ...

Logical State Representation
- State(t,1)
- State(t,2)
- State(t,3)
- State(t,4)
- ...

Annotated Business Process
- \( T_1 \)
- \( T_2 \)
- \( T_3 \)
- \( T_4 \)
- \( T_5 \)
- \( T_6 \)
- \( T_7 \)

Legalese Formalisation

Status Report

Recommendation Sub-system

Recommendations
Privacy Regorously

- collection of medical information is forbidden
  - c destruction of medical information compensates the illegal collection
    \[ r_1 : \Rightarrow [O] \neg \text{medicalInfo} \otimes [O] \text{destroy} \]
- collection of medical information is permitted if acting under a court order
  \[ r_2 : \text{courtOrder} \Rightarrow [P] \text{medicalInfo} \]
- collection of personal information is forbidden
  \[ r_3 : \Rightarrow [O] \neg \text{personalInfo} \]
- collection personal information is permitted if collection of medical information is permitted
  \[ r_4 : [P] \text{medicalInfo} \Rightarrow [P] \text{personalInfo} \]
Are We Regorously Compliant?

\[ r_1 : \Rightarrow [O]\neg medicalInfo \otimes [O]destroy \]
\[ r_2 : courtOrder \Rightarrow [P]medicalInfo \]
\[ r_3 : \Rightarrow [O]\neg personalInfo \]
\[ r_4 : [P]medicalInfo \Rightarrow [P]personalInfo \]
Are We Regorously Compliant?

State(start) : ¬courtOrder

\[ r_1 : \Rightarrow [O]¬medicalInfo \otimes [O]destroy \]
\[ r_2 : courtOrder \Rightarrow [P]medicalInfo \]
\[ r_3 : \Rightarrow [O]¬personalInfo \]
\[ r_4 : [P]medicalInfo \Rightarrow [P]personalInfo \]
Are We Regorously Compliant?

\[
\begin{align*}
T_1 & : \text{Collect Medical Information} \\
T_2 & : \text{Collect Personal Information} \\
T_3 & : \text{Destroy Medical Information}
\end{align*}
\]

\[
\begin{align*}
\text{State}(\text{start}) & : \neg \text{courtOrder} \\
\text{Force}(T_1) & : [O] \neg \text{medicalInfo} \\
& \quad [O] \neg \text{personalInfo} \\
\text{State}(T_1) & : \text{medicalInfo} \\
\text{Violated}(T_1) & : [O] \neg \text{medicalInfo} \\
\text{State}(T_2) & : \text{personalInfo} \\
\text{Violated}(T_2) & : [O] \neg \text{personalInfo} \\
\text{State}(T_3) & : \text{destroy} \\
\text{Compensated}(T_3) & : [O] \neg \text{medicalInfo}
\end{align*}
\]

\[
\begin{align*}
r_1 & : \Rightarrow [O] \neg \text{medicalInfo} \otimes [O] \text{destroy} \\
r_2 & : \text{courtOrder} \Rightarrow [P] \text{medicalInfo} \\
r_3 & : \Rightarrow [O] \neg \text{personalInfo} \\
r_4 & : [P] \text{medicalInfo} \Rightarrow [P] \text{personalInfo}
\end{align*}
\]
Are We Regorously Compliant?

\[
\begin{align*}
r_1 & : \Rightarrow [O] \neg \text{medicalInfo} \otimes [O] \text{destroy} \\
r_2 & : \text{courtOrder} \Rightarrow [P] \text{medicalInfo} \\
r_3 & : \Rightarrow [O] \neg \text{personalInfo} \\
r_4 & : [P] \text{medicalInfo} \Rightarrow [P] \text{personalInfo}
\end{align*}
\]

State(start) : $\neg \text{courtOrder}$

Force($T_1$) : $[O] \neg \text{medicalInfo}$

State($T_1$) : $\text{medicalInfo}$

Force($T_2$) : $[O] \neg \text{personalInfo}$

State($T_2$) : $\text{personalInfo}$

Force($T_3$) : $\neg \text{medicalInfo}$

State($T_3$) : $\text{destroy}$

Compensated($T_3$) : $[O] \neg \text{medicalInfo}$
Are We Regorously Compliant?

\[ r_1 : \Rightarrow [O] \neg medicalInfo \otimes [O] destroy \]
\[ r_2 : courtOrder \Rightarrow [P] medicalInfo \]
\[ r_3 : \Rightarrow [O] \neg personalInfo \]
\[ r_4 : [P] medicalInfo \Rightarrow [P] personalInfo \]

\[ State(start) : \neg courtOrder \]
\[ Force(T_1) : [O] \neg medicalInfo \]
\[ [O] \neg personalInfo \]

\[ State(T_1) : medicalInfo \]
\[ Violated(T_1) : [O] \neg medicalInfo \]
Are We Regorously Compliant?

\[ r_1: \Rightarrow [O] \neg medicalInfo \otimes [O] destroy \]
\[ r_2: courtOrder \Rightarrow [P] medicalInfo \]
\[ r_3: \Rightarrow [O] \neg personalInfo \]
\[ r_4: [P] medicalInfo \Rightarrow [P] personalInfo \]

State(start) : \neg courtOrder
Force(T_1) : [O] \neg medicalInfo
                       [P] personalInfo
State(T_1) : medicalInfo
Violated(T_1) : [O] \neg medicalInfo
Force(T_2) : [O] destroy
Are We Regorously Compliant?

\[ \begin{align*}
    r_1 : & \implies [O]\neg medical\text{Info} \otimes [O]\neg destroy \\
    r_2 : & \text{courtOrder} \implies [P]medical\text{Info} \\
    r_3 : & \implies [O]\neg personal\text{Info} \\
    r_4 : & [P]medical\text{Info} \implies [P]personal\text{Info}
\end{align*} \]

\[ \begin{align*}
    \text{State}(start) : & \neg \text{courtOrder} \\
    \text{Force}(T_1) : & [O]\neg medical\text{Info} \quad [O]\neg personal\text{Info} \\
    \text{State}(T_1) : & medical\text{Info} \\
    \text{Violated}(T_1) : & [O]\neg medical\text{Info} \\
    \text{Force}(T_2) : & [O]\text{destroy} \\
    \text{State}(T_2) : & personal\text{Info} \\
    \text{Compensated}(T_3) : & [O]\neg medical\text{Info}
\end{align*} \]
Are We Regorously Compliant?

\[ r_1: \Rightarrow [O] \neg medicalInfo \otimes [O] destroy \]
\[ r_2: courtOrder \Rightarrow [P] medicalInfo \]
\[ r_3: \Rightarrow [O] \neg personalInfo \]
\[ r_4: [P] medicalInfo \Rightarrow [P] personalInfo \]

State(start) : \neg courtOrder
Force(T_1) : [O] \neg medicalInfo
Force(T_1) : [O] \neg personalInfo

State(T_1) : medicalInfo
Violated(T_1) : [O] \neg medicalInfo

State(T_2) : personalInfo
Violated(T_2) : [O] \neg personalInfo
Are We Regorously Compliant?

\[
\begin{align*}
& r_1 : \Rightarrow [O]\neg medical\text{Info} \otimes [O]\neg destroy \\
& r_2 : court\text{Order} \Rightarrow [P]\text{medical\text{Info}} \\
& r_3 : \Rightarrow [O]\neg personal\text{Info} \\
& r_4 : [P]\text{medical\text{Info}} \Rightarrow [P]\text{personal\text{Info}}
\end{align*}
\]

\[
\begin{align*}
\text{State}(\text{start}) : & \neg court\text{Order} \\
\text{Force}(T_1) : & [O]\neg medical\text{Info} \\
& [O]\neg personal\text{Info} \\
\text{State}(T_1) : & \text{medical\text{Info}} \\
\text{Violated}(T_1) : & [O]\neg medical\text{Info} \\
\text{Force}(T_2) : & [O]\neg destroy \\
\text{State}(T_2) : & personal\text{Info} \\
\text{Violated}(T_2) : & [O]\neg person\text{al\text{Info}} \\
\text{State}(T_3) : & destroy
\end{align*}
\]
Are We Regorously Compliant?

\[
\begin{align*}
\text{State}(\text{start}) & : \neg \text{courtOrder} \\
\text{Force}(T_1) & : [O] \neg \text{medicalInfo} \quad [O] \neg \text{personalInfo} \\
\text{State}(T_1) & : \text{medicalInfo} \\
\text{Violated}(T_1) & : [O] \neg \text{medicalInfo} \\
\text{Force}(T_2) & : [O] \text{destroy} \\
\text{State}(T_2) & : \text{personalInfo} \\
\text{Violated}(T_2) & : [O] \neg \text{personalInfo} \\
\text{State}(T_3) & : \text{destroy} \\
\text{Compensated}(T_3) & : [O] \neg \text{medicalInfo}
\end{align*}
\]

\[\begin{align*}
r_1 &: \Rightarrow [O] \neg \text{medicalInfo} \otimes [O] \text{destroy} \\
\text{Start} & \rightarrow T_1 \Rightarrow \text{Collect Medical Information} \\
T_1 & \rightarrow T_2 \Rightarrow \text{Collect Personal Information} \\
T_2 & \rightarrow T_3 \Rightarrow \text{Destroy Medical Information} \\
\text{End} &
\end{align*}\]
The Regorous Evaluation

Formalised Chapter 8 (Complaints) of TCPC 2012. Modelled the compliant handling/management processes of an Australian telco.

41 tasks, 12 decision points (xor), 2 loops
shortest trace: 6 traces longest trace (loop): 33 tasks
longest trace (no loop): 22 tasks
over 1000 traces, over 25000 states
The Regorous Evaluation

TCPC 2012 Chapter 8. Contains over 100 commas, plus 120 terms (in Terms and Definitions Section). Required 223 propositions, 176 rules.

<table>
<thead>
<tr>
<th>Obligation Type</th>
<th>Count</th>
<th>(Required)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Punctual Obligation</td>
<td>5</td>
<td>(5)</td>
</tr>
<tr>
<td>Achievement Obligation</td>
<td>90</td>
<td>(110)</td>
</tr>
<tr>
<td>Preemptive</td>
<td>41</td>
<td>(46)</td>
</tr>
<tr>
<td>Non preemptive</td>
<td>49</td>
<td>(64)</td>
</tr>
<tr>
<td>Non perdurant</td>
<td>5</td>
<td>(7)</td>
</tr>
<tr>
<td>Maintenance Obligation</td>
<td>11</td>
<td>(13)</td>
</tr>
<tr>
<td>Prohibition</td>
<td>7</td>
<td>(9)</td>
</tr>
<tr>
<td>Non perdurant</td>
<td>1</td>
<td>(4)</td>
</tr>
<tr>
<td>Permission</td>
<td>9</td>
<td>(16)</td>
</tr>
<tr>
<td>Compensation</td>
<td>2</td>
<td>(2)</td>
</tr>
</tbody>
</table>
Questions?

Guido Governatori
guido.governatori@data61.csiro.au


