

Excercises “Enterprise Privacy Policies”

Excercise 1:

Describe whether below privacy preferences expressed in APPEL would or would not accept the privacy policy of www.expedia.ch (see Excercises “P3P”).

```
<appel:APPEL xmlns:APPEL="...">
  <appel:RULESET crtddb="gka" crtddon="2006-05-23">

    <appel:RULE behavior="block">
      <POLICY>
        <STATEMENT>
          <PURPOSE><contact/></PURPOSE>
          <RETENTION><indefinitely/></RETENTION>
          <CATEGORIES connective="and">
            <physical/><demographic/>
          </CATEGORIES>
        </STATEMENT>
      </POLICY>
    </appel:RULE>

  </appel:RULESET>
</appel>APPEL>
```

Solution:

Above privacy preference blocks Web sites which collect data of categories `<physical/>` and `<demographic/>` for purpose `<contact/>` and never delete it. This data is part of the statement for group “Mailing Registration” of explora.ch’s P3P policy.

```
<!-- Statement for group "Mailing registration" -->
<STATEMENT>
  <CONSEQUENCE>This information is collected so that we can send you valuable and useful
  information which is relevant to your needs and interests.</CONSEQUENCE>
  <PURPOSE><contact/><current/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><indefinitely/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#dynamic.miscdata" optional="yes">
      <CATEGORIES><physical/></CATEGORIES>
    </DATA>
    <DATA ref="#dynamic.miscdata">
      <CATEGORIES><online/></CATEGORIES>
    </DATA>
    <DATA ref="#dynamic.miscdata">
      <CATEGORIES><demographic/></CATEGORIES>
    </DATA>
  </DATA-GROUP>
</STATEMENT>
```

Thus, above privacy preference would not accept that policy.

Excercise 2:

Write in APPEL a privacy preference that would accept the P3P policy of www.expedia.ch (see Exercises “P3P”).

Solution:

```
<appel:APPEL xmlns:APPEL="...">
  <appel:RULESET crtdby="gka" crtdon="2007-04-23">

    <appel:RULE behavior="request">
      <POLICY>
        <STATEMENT>
          <PURPOSE><contact/></PURPOSE>
          <RETENTION><indefinitely/></RETENTION>
          <CATEGORIES connective="and">
            <physical/><demographic/>
          </CATEGORIES>
        </STATEMENT>
      </POLICY>
    </appel:RULE>

  </appel:RULESET>
</appel>APPEL
```

Excercise 3:

Write in APPEL a privacy preference that would block the collection of e-mail addresses if stored forever. Would this preference accept the P3P policy of www.s1rgwaedi.ch (see Exercises “P3P”)?

Solution:

```
<appel:APPEL xmlns:APPEL="...">
  <appel:RULESET crtdby="gka" crtdon="2007-04-23">

    <appel:RULE behavior="block">
      <POLICY>
        <STATEMENT>
          <RETENTION><indefinitely/></RETENTION>
          <DATA-GROUP connective="and">
            <DATA>user.home-info.online.email</DATA>
          </STATEMENT>
        </POLICY>
      </appel:RULE>

  </appel:RULESET>
</appel>APPEL
```

Above privacy preference would accept the P3P policy of `www.slrgrwaedi.ch` as the retention time stated there is `<stated-purpose/>` and thus does not match value `<indefinitely/>`.

Excercise 4:

Show that a preference to block web sites that *do not use* home telephone numbers for telemarketing is *not* robust.

Solution: Let d denote the data type of home telephone numbers and let action a denote the purpose of telemarketing. Let d' denote another data type such that $d \neq d'$. Let $f()$ denote the privacy preference.

To show:

$$\exists p_1, p_2 . p_1 \sqsubseteq p_2 \text{ and } f(p_2) \not\equiv f(p_1)$$

Above privacy preference function $f()$ can be defined as follows:

$$f(p) = \begin{cases} \text{false} & \text{if } a \notin p(d); \\ \text{true} & \text{otherwise.} \end{cases}$$

It blocks a policy p if $a \notin p(d)$ and otherwise accepts it.

$$p_1 \sqsubseteq p_2 \leftrightarrow \forall d \in D . p_1(d) \subseteq p_2(d)$$

Next we define two privacy policies p_1 and p_2 for which $p_1 \sqsubseteq p_2$ holds:

$$\begin{aligned} a &\in p_1(d') \\ a &\in p_2(d') \text{ and } a \in p_2(d) \end{aligned}$$

We see that privacy preference f accepts policy p_2 because $a \in p_2(d)$ and blocks policy p_1 because $a \notin p_1(d)$.

Excercise 5:

Please read below text from the paper of Barth and Mitchell (2005):

In the following example, Alice is the consumer and Dr. Bob is the service provider. They are concerned with the data objects blood cholesterol level, T-cell count, and blood test results. Blood test results contain both blood cholesterol level and T-cell count. They are concerned with the action “disclose X.”

Alice is HIV-positive. She wishes to keep her medical records private because she fears she will be denied health insurance if prospective insurers learn her HIV status. Conservatively, she can prohibit disclosure of her entire medical history, but she can obtain a better insurance rate if she permits certain disclosures. She is willing to disclose some of her record, such as her age, weight, and x-rays, but she does not wish to disclose results of blood tests. In evaluating privacy policies, Alice decides to ask, “Does this policy permit disclosure of blood test results?”

After framing her question, Alice consults the privacy policy of her physician, Dr. Bob, to determine if he will respect her preference to keep blood test results confidential. In his policy, Dr. Bob promises not to disclose blood cholesterol levels. This is not sufficient to satisfy Alice because it does not preclude Dr. Bob from disclosing

her T-cell count, a blood test result. Alice, therefore, concludes that Dr. Bob's policy does permit disclosure of some important blood test results.

Dr. Bob's perspective on his policy is different from Alice's perspective. In order to provide quality care for his patients, Dr. Bob wishes to disclose certain records, such as blood test results. In evaluating his privacy policy, he decides to ask, like Alice, "Does this policy permit disclosure of blood test results?" His policy promises not to disclose blood cholesterol levels, and therefore, prohibits him from disclosing blood test results in their entirety. He concludes his policy does not permit disclosure of blood test results.

Alice and Dr. Bob appear to be asking the same question, but their questions differ in their use of quantifiers. Whereas Alice is worried about Dr. Bob disclosing part of her blood test results, Dr. Bob is worried about respecting each of his promises about blood test results. Reformulate the questions of Alice and Dr. Bob in such a way that they lead to different answers.

Solution:

Alice: Does the privacy policy allow disclosure of *any* blood test results?

blood test result $\Vdash_p \diamond$ disclose

Dr. Bob: Does the privacy policy allow disclosure of *all* blood test results?

blood test result $\Vdash_p \square$ disclose