Privacy Policies

Naranker Dulay

n.dulay@imperial.ac.uk
https://www.doc.ic.ac.uk/~nd/pet

Website Privacy Policies

- Most websites have a privacy policy/statement/notice somewhere on their website - typically a tiny link at the bottom of the homepage.
- These aim to inform visitors about the site's data-handling practices. Visitors are supposed to read them and decide whether to use the site (consent is often implicit if the site is used).
- No one ever reads them! Often written by lawyers. Average length ~2500 words.
- Imperial College (26 November 2018)
  https://www.imperial.ac.uk/about-the-site/privacy/
- Google UK (26 November 2018)
  https://policies.google.com/privacy?hl=en&gl=uk
- Apple UK (26 November 2018)
  https://www.apple.com/uk/legal/privacy/en-ww/
- Amazon (26 November 2018)
  https://www.amazon.co.uk/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=201909010
- Facebook (26 November 2018)
  https://www.facebook.com/privacy/explanation

What tech CEOs think

- **Scott McNealy**, Co-founder, Sun Microsystems, 1999

  You have zero privacy anyway. Get over it.

- **Eric Schmidt,** CEO, Google

  If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.

  We know where you are. We know where you've been. We can more or less know what you're thinking ...

  Just remember when you post something, the computers remember forever.

- **Mark Zuckerberg**, CEO, Facebook

  Our work to improve privacy continues today.

- **Steve Jobs**, Co-Founder, Apple

  We've always had a very different view of privacy than some of our colleagues in the [Silicon] Valley. We take privacy extremely seriously....
  A lot of people in the Valley think we're really old fashioned about this.

GDPR - General Data Protection Regulation

- **What**

  Wide ranging regulation governing data privacy – data related to living persons
  Improved rights for individuals
  New obligations on organisations

- **Why?**

  Organisations did not take data privacy responsibilities seriously enough.
  Potential for **very large fines** for serious infringements. Upto €20M or 4% of worldwide turnover, whichever is greater

- *Although written in plain English, the regulation is a legal document written for lawyers and judges to interpret not a specification for computer scientists* :-(

Rights of Individuals

- Right of **access** – within 1 month
- Right of **rectification** – correction or erasure of inaccurate data
- Right to **data portability** – provision of data in machine-readable format
- Right to **transparency** – typically via privacy notices
- Right to **object** to processing for the purpose of **direct marketing**

Conditional rights

- Right to **erasure** - the so-called **right to be forgotten**
- Right not be subject to **automated decision-making**
- Right to **restrict processing**
- Right to **object if processing** was in public interest, or legitimate interests of organisation
- Right to **object to processing** for scientific, historical or statistical purposes

Legal Basis

There are 6 lawful bases for the collection of personal data under GDPR:

1. Necessary for **execution of contract** with data subject e.g. employment contract
2. Necessary for **compliance with a legal obligation** e.g. tax reporting
3. Performance of **task carried out in the public interest** e.g. research will normally be considered in the public interest where data is not sensitive. ***Sensitive personal data*** includes medical/health data, racial/ethnic origin, political views, religious beliefs, trade union membership. This basis is possible even for sensitive personal data if additional conditions/safeguards are met.
4. fulfil the **legitimate interests of the organisation**, except where overridden by rights and freedoms of individuals
5. protect **vital interests of individuals** (typically life-or-death scenarios)
6. **subject has given consent** – at least 8 obligations need to be met for this basis, organisations will try to adopt one of the other bases above if possible.

There are also **exemptions** e.g. for national security.

Example - Consent

- Where processing is based on consent, the controller shall be **able to demonstrate** that the data subject has consented to processing of his or her personal data.

- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

- The data subject shall have the right to **withdraw his or her consent at any time.** The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

- When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Consent

- **Freely given**
- **Specific**
- **Informed**
- **Provided by an appropriate method**
- **Not silence or a pre-ticked box**
- **Distinguishable from other matters**
- **Can be evidenced**
- **Can be withdrawn**

P3P (Platform for Privacy Preferences) Policies

- W3C recommendation (2002).
- Allowed websites to disclose privacy policies in machine-readable format (XML). Policies could be associated with site, pages, or elements on page.
- Policies included (i) contact info, (ii) type of access, (iii) dispute resolution procedure, (iv) data collected, (v) uses, (vi) opt-in/out, (vii) retention
- P3P clients (typically web browsers) could request policies and compare them with the user's preferences (IE6 used a privacy-tab slider and generated privacy-summary report).
- P3P clients could also detect policy changes e.g. is policy different from last version downloaded.
- Requirement that P2P policies be consistent with natural language ver.

- ***P3P limitations***
- **Didn't capture user preferences**. Left to clients (APPEL never adopted).
- No enforcement mechanisms. No legal standing.
- Often complex and nuanced.
- Didn't capture positive promises.
- Couldn't express many reasonable natural language policies. Couldn't cope with mixed policies - regulatory, organisational, application-level.
- Informing users remained challenging.
- Companies had strong economic reasons to collect and aggregate personal data.
- Abandoned.

Privacy Policies

- **Service Provider Privacy Policy**
  A statement that defines how a service provider gathers, uses, discloses and manages an individual's data.
- **User Privacy Policy (Privacy Preferences)**
  A statement that defines how an individual would like a service provider (third party) to use their data, particularly personal data.

Issues

- How to decide whether a service provider's privacy policy satisfies a user's privacy policy?
- How to enforce compliance of the user's privacy policy by the service provider?
- How to handle a user's or regulator's anonymisation requirements?
- How to *negotiate* privacy-terms if policies conflict?
- How to define sharing rules for friends/family/collaborators/strangers etc.

S4P Language Goals

- **Declarative.** Defines policies, not how to enforce them
- **Generic.** Semantics of services are hidden with abstraction
- **Reasoning.** Able to check if a service policy satisfies a user policy (preference).
- **Expressive**. Supports parameterised (reusable) policies, hierarchical specification, complex (fine-grained) constraints.
- **Delegation**. Supports delegation of authority.
- **Readable policies** (debatable)
- **Enforceable policies.** Enforcement could be via static analysis, runtime monitoring, audit trails.

- Assumes users trust service providers to enforce the user's policies.
- Prototype implemented in SecPAL engine extended with may/will constructs. Uses Datalog and a resolution algorithm with tabling. Successful queries can be visualised with a proof viewer. Failed queries can be analysed using abduction tool.
- Supports **policy evolution**, i.e. can check that a new service policy satisfies existing user preferences.
- Show which queries are true, should user agree to disclose data.
- Show satisfaction checking algorithm is correct.

S4P Syntax

Both a **user privacy preference** and **service privacy policy** consist of a set of assertions and a query.

Assertion

```
E says f0 if f1, .., fn where c
```

Delegation of authority

Fact

```
f ::= a | e may b | e will b | e can say f
```

Query

```
q ::= e says f? | c? | ¬q | q1 ∧ q2 | q1 ∨ q2 | exists x: q
```

E	constant	Typically **principals** e.g. Alice, Bob, Service Provider
x	variable	
e	expression	**Constant** or **variable**
c	constraint	Constraint on variables occurring in assertion
a	atom	**Predicate** written in *infix* notation e.g. 'Alice is a nicePerson'
b	behaviour atom	**Service behaviours** e.g. 'delete email within 1 yr'

Permissions and Promises

Both user privacy preferences and service privacy policies consist of a set of assertions and a query.

	Permission	**Promise**
User Preference	`may` assertion *User gives permission*	`will` query *User asks for promise*
Service Policy	`may` query *Service asks for permission*	`will` assertion *Service gives promise*

User Preference may assertion (You may)

Expresses what a service `may` do with the user's data (permissions).

User Preference will query (Will you)

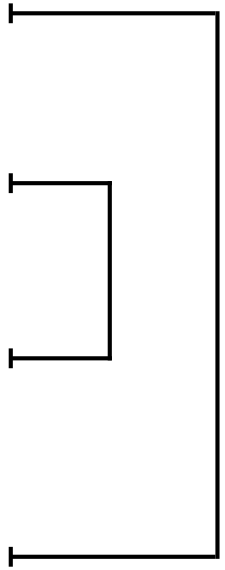
Expresses behaviours that a service `will` (must) exhibit (promises).

Service Provider Policy will assertion (I will)

Expresses behaviours that a service `will` do (promises)

Service Provider Policy may query (May I)

Expresses what a service `may` do with the user's data (permissions)



Example 1: User Alice's Privacy Preference

Service Provider <SP> will be instantiated during policy evaluation e.g. to Bob.

```
A1  Alice says     <SP> may 'use EmailAddr for purpose'
                   if '<SP> is a TravelAgent'
                   where purpose not in {Marketing, Statistics}

A2  Alice says     <SP> may 'delete EmailAddr within t'
```

```
A3  exists t:      <SP> says <SP> will 'delete EmailAddr within t'? ∧
                   t <= 30 days?
```

A1 Alice gives Service Providers that are travel agents permission to use her Email address provided the purpose of the Email is not Marketing and is not Statistics.

A2 Alice gives Service Providers permission to delete her email. A2 doesn't require them to however (see A3).

A3 Alice requires Service Providers to delete her email address within 30 days. A3 does not permit them to however (see A2).

Example 1: Service Provider Bob's Privacy Policy

<User> will be instantiated during policy evaluation e.g. to Alice.

B1 `Bob says Bob will 'delete EmailAddr within 7 days'`

B2 `<User> says Bob may 'use EmailAddr for News'? ∧`
`<User> says Bob may 'delete EmailAddr within 7days'?`

B1 Bob promises to delete Email addresses within 7 days.

B2 Bob requires <User> permission to use the Email address for News and
Bob requires <User> permission to delete the Email addresses with 7 days.

Case Study

- **Alice's Privacy Preference.** Alice cares about online child protection.
- Alice requires SP to allow her to edit parental control settings (A1)
- Alice requires SP to comply with Children's Online Privacy Protection Act (COPPA). Delegates compliance to schemes approved by FTC (A2, A3).
- Has a statement from FTC that TrustE is compliant scheme (A4)
- Cookies are allowed provided they're revoked with 4 years (A5, A6, A8)
- SP permits Alice to perform actions on objects (A7).
- Alice asserts that she uses MSN client version 9.5 (A9)

- **Microsoft Privacy Policy (2010).**
- TRUSTe asserts Microsoft complies with COPPA (M0).
- The conditions when parental controls can be edited are defined by M1-M4.
- The different types of membership are delegated to MSN (M5).
- MSN asserts that Alice has a MSNpremium account (M6)
- Microsoft trusts users who say that they are using a particular version of the MSNClient (M7)
- Microsoft assert they delete cookies within 2 years (M8).
- Permission Microsoft requests of user for this (M9).

Alice's Privacy Preference

A1	⟨SP⟩ says Alice says	⟨SP⟩ will 'allow ⟨User⟩ to Edit ParentalControls'? ∧ '⟨SP⟩ complies with COPPA'?
A2	Alice says	x can say 'y complies with COPPA' if 'y is member of COPPACompliancySchemes'
A3	Alice says	FTC can say 'x is a member of COPPACompliancySchemes'
A4	FTC says	'TRUSTe is a member of COPPACompliancySchemes'
A5	Alice says	⟨SP⟩ may 'use Cookies for x' if ⟨SP⟩ will 'revoke Cookies within t' where t ≤ 5yr
A6	Alice says	⟨SP⟩ can say ⟨SP⟩ will 'revoke Cookies within t'
A7	Alice says	⟨SP⟩ may 'allow Alice to *action object*'
A8	Alice says	⟨SP⟩ may 'revoke Cookies within t'
A9	Alice says	'Alice is using MSNClient version 9.5'

Microsoft's Privacy Policy

Microsoft

M0 TRUSTe says 'MS complies with COPPA'

M1 MS says MS will 'allow ⟨User⟩ to Edit ParentalControls'
if '⟨User⟩ is member of *msntype*,
msntype supports parental controls,
⟨User⟩ is using software MSNClient version v'
where $v \leq 9.5$

M2 MS says 'MSNPremium supports parental controls'

M3 MS says 'MNSPlus supports parental controls'

M4 MS says 'MSN9DialUp supports parental controls'

M5 MS says MSN can say 'x is member of
{MSN', MSNPremium',MSNPlus', MSN9DialUp}'

M6 MSN says 'Alice is member of MSNPremium'

M7 MS says ⟨User⟩ can say '⟨User⟩ is using MSNClient version v'

M8 MS says MS will 'revoke Cookies within 2yr'

M9 ⟨User⟩ says MS may 'use Cookies for AdTracking'? ∧
⟨User⟩ says MS may 'revoke Cookies within 2yr'? ∧
⟨User⟩ says MS may 'allow ⟨User⟩ to Edit ParentalControls'?

Policy Satisfaction

- Does Microsoft's Privacy Policy satisfy Alice's Privacy Preference?
- We need to check Alice's `will` query (A1) and Microsoft's `may` query (M9) against all the assertions (A2-A9, M0-M8). After instantiating `<SP>` and `<User>` we have

```
A1  MS says     MS will 'allow Alice to Edit ParentalControls'? ∧
Alice says      'MS complies with COPPA'?
```

- First part of A1 is satisfied by:

```
M1  MS says     MS will 'allow Alice to Edit ParentalControls'
                if 'Alice is member of msntype,
                    msntype supports parental controls,
                    Alice is using software MSNClient version v'
                where v ≤ 9.5
M6  MSN says    'Alice is member of MSNPremium'
M5  MS says     MSN can say 'x is member of
                     {MSN', MSNPremium',MSNPlus', MSN9DialUp}'
M2  MS says     'MSNPremium supports parental controls'
A9  Alice says 'Alice is using MSNClient version 9.5'
M7  MS says     Alice can say 'Alice is using MSNClient version v'
```

Policy Satisfaction 2

Microsoft

- Does Microsoft's Privacy Policy satisfy Alice's Privacy Preference?
- We need to check Alice's will query (A1) and Microsoft's may query (M9) against the all assertions (A2-A9, M0-M8). After instantiating `<SP>` and `<User>` we have

```
A1 MS says      MS will 'allow Alice to Edit ParentalControls'? ∧
Alice says      'MS complies with COPPA'?
```

- Second part of A1 is satisfied by:

```
M0  TRUSTe says 'MS complies with COPPA'
A4  FTC says    'TRUSTe is a member of COPPACompliancySchemes'
A3  Alice says  FTC can say 'TRUSTe is a member of
                    COPPACompliancySchemes'
A2  Alice says   FTC can say 'TRUSTe complies with COPPA'
                 if 'TRUSTe is a member of COPPACompliancySchemes'
```

Policy Satisfaction 3

Microsoft

- Does Microsoft's Privacy Policy satisfy Alice's Privacy Preference?
- We also need to check Microsoft's may query (M9) against the all assertions (A2-A9, M0-M8). After instantiating <SP> and <User> we have:

```
M9  Alice says    MS may 'use Cookies for AdTracking'? ∧
    Alice says    MS may 'revoke Cookies within 2yr'? ∧
    Alice says    MS may 'allow Alice to Edit ParentalControls'?
```

- First part is satisfied by:

```
A5  Alice says    MS may 'use Cookies for AdTracking'
                  if MS will 'revoke Cookies within t' where t ≤ 5yr
A6  Alice says    MS can say MS will 'revoke Cookies within t'
M8  MS says       MS will 'revoke Cookies within 2yr'
```

- Second part is satisfied by:

```
A8  Alice says    MS may 'revoke Cookies within t'
```

- Third part is satisfied by:

```
A7  Alice says    MS may 'allow Alice to Edit ParentalControls'
```

Final Plaintexts