

Capabilities and Limitations of P3P

Girma Nigusse *Bart De Decker*

Report CW539, May 2009



Katholieke Universiteit Leuven
Department of Computer Science

Celestijnenlaan 200A – B-3001 Heverlee (Belgium)

Capabilities and Limitations of P3P

Girma Nigusse *Bart De Decker*

Report CW 539, May 2009

Department of Computer Science, K.U.Leuven

Abstract

In the last years, various privacy protection organizations formulate fair data practice principles, guidelines, model codes, and legislations [1] [2] [3] [4] [9] [10] [11] [12] [13] [14]. Following that, a number of privacy policy creation, communication, and enforcement languages, such as P3P [5], XACML [6], EPAL [7], and APPEL [8], have been developed to address the notions of these formulations. However, there is a lack of an in-depth assessment of the capabilities and limitations of these policy languages based on the fair data practice formulations. Hence, this report compares and contrasts four well formulated fair data practice principles and introduces comprehensive yet generic fair data practice requirements. Using these requirements the report makes an in-depth analysis of the capabilities and limitations of the P3P policy language. Also motivates the use of these requirements to analyze the capabilities and limitations of other privacy policy languages.

Keywords : P3P, Privacy Policies, Privacy Policies Requirements

Contents

1	Fair Data Practice Formulations	3
1.1	Selected Fair Data Practice Formulations	3
1.1.1	CFIPP	3
1.1.2	OECD Guidelines	4
1.1.3	MCPPI Model Codes	5
1.1.4	E.U. DPD	6
1.2	Generic Fair Data Practice Requirements	7
1.2.1	Notice	7
1.2.2	Consent	9
1.2.3	Access to Rectify, Erase, or Block	12
1.2.4	Data Quality	13
1.2.5	Security	14
1.2.6	Enforcement	15
2	Privacy Policy Languages	17
2.1	P3P	17
2.2	XACML	18
2.3	EPAL	19
2.4	APPLE	20
3	P3P	21
3.1	Retrieving P3P Policy	21
3.2	Elements of P3P Enabled Web Site	22
3.3	P3P Policy File	23
3.4	P3P User Agents	24
3.5	Built-In P3P User Agents	25
3.6	Privacy Bird	26
3.7	Privacy Seals	27

VI Contents

4	Evaluating P3P	29
4.1	Capabilities	29
4.2	Limitation	30
5	Concerns, Discussions, and Future Work	33
5.1	Concerns	33
5.2	Discussion	34
5.3	Future Work	35
A	Fair Data Practice Principles	37
A.1	OECD Guidelines	37
A.2	Canadian MCPPI	38
A.3	U.S. and E.U. Safe Harbor Principles	39
B	P3P Examples	41
B.1	Example P3P Policy	41
B.2	Example P3P Compact Policy	45
	References	47

List of Figures

1.1	Similarities between CFIPP and OECD	5
1.2	Similarities between OECD and MCPPI.....	6
1.3	Similarities among E.U. DPD, OECD, and MCPPI	7
1.4	Notice related interactions	8
1.5	Consent related interactions	11
1.6	Access related interactions.....	12
1.7	Data quality related interactions	13
1.8	Security related interactions	14
1.9	Enforcement related interactions	15
3.1	Retrieving P3P policy.....	22
3.2	Internet Explorer 7, cookie filtering slider.....	25
3.3	Privacy icon in Microsoft Internet Explorer 7	26
3.4	Privacy Bird indicator icons	27
3.5	TRUSTe and BBBOnline privacy seals	28
3.6	The first E.U. [EuroPriSe] privacy seal for ixquick	28

List of Acronyms

APPEL	A P3P Preference Exchange Language
Art.	Articles
CFIPP	Code of Fair Information Practice Principles
E.U. DPD	European Union Data Protection Directive
EPAL	Enterprise Privacy Authorization Language
HEW	U.S. Department of Health, Education, and Welfare
HTTP	Hypertext Transfer Protocol
LEA	Legal Enforcement Agency
MCPPI	Model Code for the Protection of Personal Information
OASIS	Advanced Open Standards for the Information Society
OECD	Organization for Economic Co-operation and Development
P3P	Platform for Privacy Preference
PICS	Platform for Internet Content Selection
PEP	Policy Enforcement Point
Sec.	Sections
SP	Service Provider
TTP	Trusted Third Party
U	User
W3C	World Wide Web Consortium
XACML	eXtensible Access Control Markup Language

Fair Data Practice Formulations

The 1973 *U.S. Department of Health, Education, and Welfare (HEW) Code of Fair Information Practice Principles* (CFIPP) [1] becomes a foundation for today's privacy friendly data practice¹ and Web site's privacy policy formulations. CFIPP influences a number of successor data practice guidelines, model codes and legislations, such as [2], [3], and [4]. Since then, a number of policy languages, such as *Platform for Privacy Preference (P3P)* [5], *eX-tensible Access Control Markup Language (XACML)* [6], *Enterprise Privacy Authorization Language (EPAL)* [7] and *A P3P Preference Exchange Language (APPEL)* [8], are introduced to automate the creation, communication, and enforcement of privacy policies.

1.1 Selected Fair Data Practice Formulations

This section compares CFIPP with three other fair data practice formulations; namely the 1980 codified *Organization for Economic Co-operation and Development (OECD) eight guidelines* [2], the 1996 Canadian standard association *Model Code for the Protection of Personal Information (MCPPI)* [3] and the 1995 *European Union Data Protection Directive (E.U. DPD)* [4]. Besides these formulations, there are a number of other data practice formulations, such as [9], [10], [11], [12], [13] and [14], which are not covered in this report.

1.1.1 CFIPP

The original CFIPP states the following five fair data practice principles.

1. *“There must be no personal data record keeping systems whose very existence is secret”.*
2. *“There must be a way for an individual to find out what information about him is in a record and how it is used”.*

¹ In literature data practice is sometimes referred to as information practice.

3. “*There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent*”.
4. “*There must be a way for an individual to correct or amend a record of identifiable information about him*”.
5. “*Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data*”.

CFIPP denounces covert *private data* collection. It recommends service providers to be open regarding their data practices, which includes letting users know what *private data* is collected from them, how that data is (going to be) used, and allow users to amend or correct their own *private data*. CFIPP also discusses purpose limitation, and obliges service providers to maintain the accuracy and *security* of *private data* collected from their users. Most importantly, CFIPP promotes data minimization by discouraging an aggressive collection of *private data* with out an intended use. Even if the CFIPP pioneers fair data practice formulations, in comparison with other successor data practice guidelines, model codes, and legislations, it addresses only basic privacy protection matters.

1.1.2 OECD Guidelines

The OECD guidelines specify privacy-aware guidelines for trans-border flow of personal data among OECD member nations [2]. The eight OECD guidelines include:

1. Collection limitation principle
2. Data quality principle
3. Purpose specification principle
4. Use limitation principle
5. Security safeguards principle
6. Openness principle
7. Individual participation principle
8. Accountability principle

Unlike CFIPP that denounces covert data collection, the OECD collection limitation principle approves covert data collection where appropriate (*see* Appendix A.1). In its use limitation principle, OECD approves the use of personal data for unstated purposes without the *consent* of the user, if it is for legitimate purpose (such as authority of law or prosecution). In comparison with CFIPP, the OECD guidelines addresses additional privacy protection matters, such as fair and lawful personal data collection, data practice openness, and accountability for stated data practice promises. In practice, on-line service providers comply with the openness principle by publishing their privacy policies on their Web sites (*see* Section 3.1). Fig. 1.1 shows which

particular OECD guidelines are similar to CFIPP. In the figure, a gray box indicates the new contribution made by the OECD guidelines, in comparison with the CFIPP. The number in the Figure indicate the list number of the CFIPP and OECD guidelines as expressed in this report.

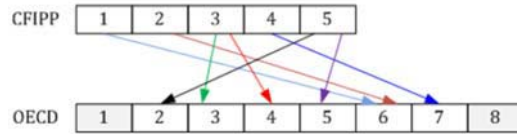


Fig. 1.1. Similarities between CFIPP and OECD

1.1.3 MCPPI Model Codes

The Canadian standard association MCPPI [3] is a *voluntary* national standard that attempts to create a balance between service provider’s *private data* needs to provide their service and user’s desire to get those services anonymously. In 1996, the Canadian Standard Association outlines the MCPPI model codes as a collection of *minimum* requirements for the protection *private data*. Thus, service providers are encouraged to *tailor* it, to meet their specific privacy requirements. The ten MCPPI interrelated *private data* fair-handling practice model codes include:

1. Accountability
2. Identifying purpose
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenge compliance

As shown in Fig. 1.2 except the introduction of limiting data retention, limiting data disclosure, and challenging compliance model codes, the MCPPI model codes are highly analogous to the OECD guidelines (and transitively to CFIPP) (*see* Appendix A.2). Fig. 1.2 shows which OECD principles are similar to which particular MCPPI model codes.

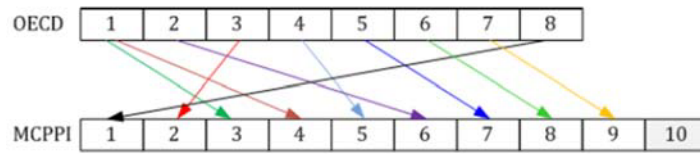


Fig. 1.2. Similarities between OECD and MCPPI

1.1.4 E.U. DPD

The 1995 E.U. DPD includes a number of privacy protection *Articles* (Art.) that intend to protect the fundamental rights and freedom of the E.U. citizens, regarding the transfer, processing, and use of *private data* locally and among E.U. member nations. The 'core' *private data* related *Sections* (Sec.) of the E.U. DPD legislation include:

1. Principles relating to data quality {Sec. 1 Art. 6}
2. Criteria for making data processing legitimate {Sec. 2 Art. 7}
3. Special categories of processing {Sec. 3 Art. 8-9}
4. Information to be given to the data subject {Sec. 4 Art. 10-11}
5. The data subjects right of access to data {Sec. 5 Art. 12}
6. Exemptions and restrictions {Sec. 6 Art. 13}
7. The data subjects right to object {Sec. 7 Art. 14-15}
8. Confidentiality and security of processing {Sec. 8 Art. 16-17}
9. Notification {Sec. 9 Art. 18-21}
10. Judicial remedies, liability and sanctions {Sec. 10 Art. 22-24}
11. Transfer of personal data to a third countries {Sec. 11 Art. 25-26}

The E.U. DPD is the only comprehensive data practice formulation. it introduces a number of new perspectives for the protection of *private data* such as the one in Art. 8-9, 13-15, and 25-26. However, as shown in Fig. 1.3, the rest of the articles in the directive exhibits similarities to previously discussed *private data* protection formulations.

In Art. 8, the E.U. DPD prohibits the processing of *special categories* of *private data*, such as ethnic origin, political view, religious view, philosophical beliefs, trade-union membership, health data, and sec life (*see* [4] Art. 8)². On compelling legitimate grounds, Art. 12 grants the data subject the right to object the processing of *private data* relating to him (*see* [4] Art. 12). Art. 25 formulate restrictive regulation regarding the transfer of E.U. citizen's *private data* to third-countries (non-E.U. countries) (*see* [4] Art. 25).

For instance, the E.U. Safe Harbor framework [15] is designed to regulate the transfer of *private data* from E.U. to U.S.-based service providers. The framework specifies a set of standards the U.S.-based service providers

² Readers are encouraged to consult the full text of the directive from [4].

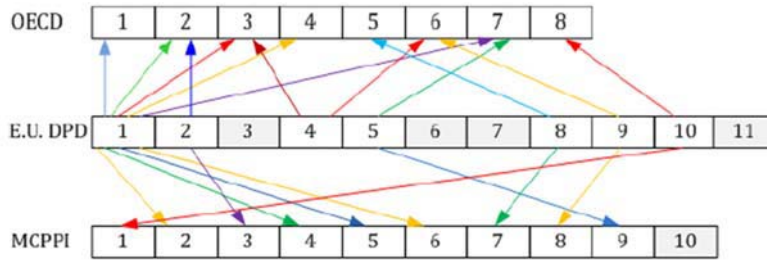


Fig. 1.3. Similarities among E.U. DPD, OECD, and MCPPI

must meet to comply with the E.U. data protection ‘adequacy’ standards (see Appendix A.3)

1.2 Generic Fair Data Practice Requirements

This section explains comprehensive yet generic data practice requirements classified into six parts: *notice*, *consent*, *access*, *data quality*, *security*, and *enforcement*. These requirements as a whole or in part can be used to design or evaluate privacy policy creation, communication, and enforcement schemes. They can also be used to evaluate the completeness of Web site’s privacy policies and the capabilities and limitations of existing privacy policy languages (see Chapter 4). The functionality of existing privacy policy user agents (see Section 3.4) and enterprise *private data* management solutions (see Section 2.2 and 2.3) can also be evaluated with this generic requirements.

1.2.1 Notice

A *notice* includes a set of data practice promises and/or declarations of a particular service provider. For instance, a *notice* statement may state that “service provider x does not share its user’s *private data* with third parties” which is a *promise* or “service provider y shares its user’s *private data* with third parties” which is a *declaration*.

(1) $U \leftarrow SP$: request(privacy policy)
(2) $U \rightarrow SP$: <i>notice</i> \leftarrow privacy policy (promises and/or declarations)

Table 1.1. Generic notice protocol

As shown in Table 1.2, a simplified *notice* protocol consists of two roles; a *User* (U) and a *Service Provider* (SP). In the protocol, the service provider’s privacy policy communicated unidirectionally to a user. Thus, data practice

notice (or Web site’s privacy policy) *are not negotiable*. Even if the user’s privacy preferences do not match with the provided service provider’s *notice* statements, the service provider do not negotiate to alter those unfriendly *notice* statement.

As depicted in Fig. 1.4 a *notice* protocol should incorporate two additional players; a *Trusted Third Party* (TTP) and *Legal Enforcement Agency* (LEA). The TTP is required to establish a trusted relationship between the user and the service provider, by certifying data practice *notice* statements. LEA should also validate the service provider’s data practice *notice* statements and the TTP certification procedures.

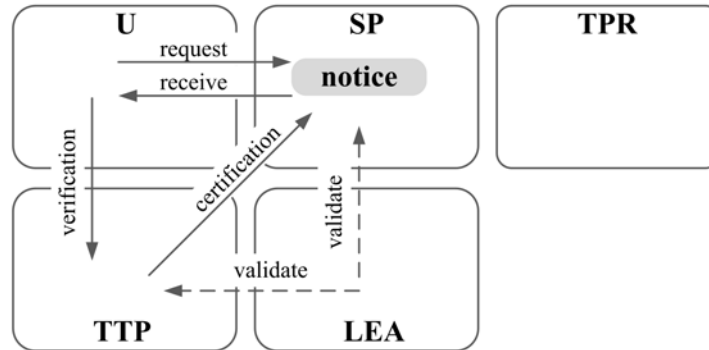


Fig. 1.4. Notice related interactions

Requirements

- **NR 1. Availability:** The service provider’s data practice *notice* should be readily available, either in human or machine-readable format or both.
- **NR 2. Assurance:** To make sure that the service provider’s actual data practice matches with its published data practice *notice* statements, its *notice* statements should be certified by a TTP.
- **NR 3. Coverage:** The set of a given data practice *notice* should encompass at least the following statement.
 - **NR 3.1 Identification:** Service providers should disclose their identification data to their users. Such identification data should at least contain the name and address of the service provider or its representative. {cf. CFIPP 1, E.U. DPD Art. 10, 11, and 19.}
 - **NR 3.2 Collection:** Service providers should justify whether their *private data* collection schemes are lawful and fair. They should also

- clearly explain which particular active and/or passive³ data collection schemes they are using. {cf. OECD 1, MCPPI 4, E.U. DPD Art. 6.}
- **NR. 3.3 Content:** Service providers should indicate the list of *private data* they intend to collect. If their list contains special data, such as data that reveal user’s racial origin, political opinions, beliefs, health data, or sex life, such collection should be explained unambiguously⁴. {cf. E.U. DPD Art. 19.}
 - **NR 3.4. Purpose:** Service providers should present an explicit and legitimate purpose to collect the user’s *private data*. {cf. OECD 3, MCPPI 2, E.U. DPD Art. 6, 18, and 19.}
 - **NR 3.5 Retention:** Service providers should clearly state for how long they intend to retain the user’s *private data* after collection. {cf. MCPPI 5, E.U. DPD Art. 6.}
 - **NR 3.6 Sharing:** Service providers should explain whether they intend to share the user’s *private data* to *Third Party Recipient* (TPR) or not. If they do share it, they should clearly identify the TPR⁵ {cf. aceu Art. 10, 11, 18, and 19.}
 - **NR 3.7 Rectification, Erasure, or Blocking:** Service providers should clearly state whether data rectification, erasure, or blocking are allowed or not, after *private data* collection. {cf. CFIPP 4 and 5, OECD 7, MCPPI 9, E.U. DPD Art. 10 and 11.}
 - **NR 3.8 Security:** Service providers should explain how they intend to maintain the *security*, i.e. the confidentiality, and integrity of the user’s *private data* after it is being collected. {cf. CFIPP 5, OECD 5, MCPPI 7, E.U. DPD Art. 8.}
 - **NR 3.9 Accountability:** Service providers should clearly state to what extent they are responsible for or legally-bound to all the promises they have made. {cf. OECD 8, MCPPI 1, E.U. DPD Art. 22, 23, and 24.}

1.2.2 Consent

[2] [3] [4] states that prior to any *private data* collection, service providers should request the *consent* of the data subject. These formulations also express exceptional conditions where service providers are not obliged to get the user’s

³ Passive data collection schemes uses hidden electronic monitoring techniques to collect user’s *private data*, such as cookies. Whereas, active data collection schemes uses interactive techniques, such as Web forms, and prompt users to disclose their *private data*.

⁴ E.U. DPD Sec. 3 Art. 8.1 prohibits the processing of *private data* that may reveal the user’s ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, health data, or sex life.

⁵ When E.U. citizen’s *private data* involved and if the TPR is from a third country (i.e. a service provider from non-E.U. countries), it is necessary to make sure and express that the recipient meets the E.U. DPD privacy requirements).

consent. For instance, service providers are not required to get the user’s *consent* when the *private data* collection is for national security, prevention, investigation, detection, or prosecution of criminal offenses (cf. [4] Sec. 6 Art. 13).

<p>Scenario 1 : Where requesting the user’s <i>consent</i> is inappropriate.</p> <p>(1) $U \leftarrow SP : request(pd_1, pd_2, pd_3, \dots pd_n)$</p> <p>(2) $U \rightarrow SP : reveal(pd_1, pd_2, pd_3, \dots pd_n)$</p>
<p>Scenario 2 : Where requesting the user’s <i>consent</i> is appropriate.</p> <p>(1) $U \leftarrow SP : requestConsent(pd_1, pd_2, pd_3, \dots pd_n)$</p> <p>(2) $U \rightarrow SP : priConsent \leftarrow consent(pd_{2_1}, pd_{4_2}, pd_{6_3}, \dots pd_{n_m})$ where $(m \leq n)$</p> <p>(3) $U \leftarrow SP : request(pd_{2_1}, pd_{4_2}, pd_{6_3}, \dots pd_{n_m})$ where $(m \leq n)$</p> <p>(4) $U \rightarrow SP : reveal(pd_{2_1}, pd_{4_2}, pd_{6_3}, \dots pd_{n_m})$ where $(m \leq n)$</p> <p>(5) $SP : use(pd_{2_1}, pd_{6_2}, \dots pd_{n_m})$ where $(m \leq n)$ w.r.t. the user <i>priConsent</i></p>
<p>Scenario 3 : Where requesting the user’s <i>consent</i> is appropriate and when the collected user’s <i>private data</i> is intended to be used under previously unexpressed conditions.</p> <p>(1) $U \leftarrow SP : requestConsent(pd_{2_1}, pd_{4_2}, pd_{6_3}, pd_{8_4}, \dots pd_{n_k})$ where $(k \leq n)$</p> <p>(2) $U \rightarrow SP : secConsent \leftarrow consent(pd_2, pd_4, \dots pd_n)$</p> <p>(3) $SP : (use(pd_{2_1}, pd_{4_2}, \dots pd_{n_k})$ w.r.t. the user <i>secConsent</i>) \vee $(use(pd_{6_1}, pd_{8_2}, \dots pd_{n_m})$ w.r.t. the user <i>priConsent</i> \wedge (<i>destroy</i> $(pd_{6_1}, pd_{8_2}, \dots pd_{n_m}) \leftarrow if(!secConsent)))$ where $(k \leq n), (m \leq n)$</p>

Table 1.2. Generic consent protocol

As shown in the generic *consent* protocol (Table 1.2 and Fig. 1.5), a user *consent* should be requested prior to *private data* ($pd_1, pd_2, pd_3, \dots pd_n$) collection. This type of *consent* is primarily required for first time *private data* collection and we call it *primary consent* (*priConsent*). Moreover, service providers might intend to use or manipulate already collected user’s *private data* for unstated purposes *internally* or *externally*. For instance, *private data* collected for delivery can be used for targeting marketing, *private data* to be kept for two years might be retained for more years, or *private data* to be shared by expressed TPR might be shred with other TPR. When a service provider changes its prior data practice policies, further manipulation of user’s *private data* is likely. For instance, changes of the controller’s identity, changes in collection means, changes of collection purpose, changes of retention policy, changes of TPR (changes in sharing policy), changes in *access* policy, or changes in accountability policy, requires an additional user *consent* and we call it *secondary consent* (*secConsent*). Unlike the *notice* protocol, the *consent* protocol is bidirectional. It requires an interaction between a user and a service provider, thus it necessitates negotiation.

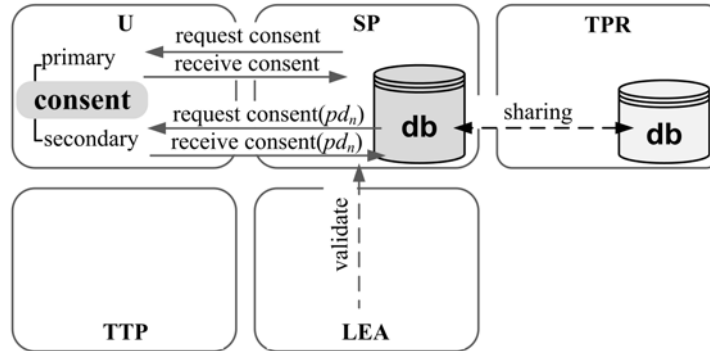


Fig. 1.5. Consent related interactions

Consent Requirements:

- CR 1. Primary Consent:** The user's *consent* is required prior to any *private data* collection, except where inappropriate. {cf. OECD 1, MCPPI 3, E.U. DPD Art. 7 and 8.}

 - Special Case 1:** Processing of special *private data* that includes the racial origin, political opinions, beliefs, health, sex life, etc, of a user is prohibited. However, such data may be collected when the data subject has given his/her explicit *consent*. {cf. E.U. DPD Art. 8.}
 - Exception 1:** The right to *priConsent* may be restricted (or not necessarily required) when the purpose of collection related to national security, defense, public security, criminal offenses, breaches of ethics for regulated profession, financial interest of the E.U., for the protection of the data subject or of the rights and freedoms of others. {cf. E.U. DPD Art. 13.}
- CR 2. Secondary consent:** The knowledge and *consent* of users are required for further manipulation⁶ of collected *private data*, except where inappropriate.

 - CR 2.1 Authentication:** A service provider should authenticate the user before requesting *secConsent*, to validate whether the *private data* belongs to that user or not.
 - Exception 1:** A *secConsent* is not required if the *private data* is further processed for historical, statistical, or scientific purposes. {cf. E.U. DPD Art. 6.}
 - Exception 2:** The right to *priConsent* may be restricted (or not necessarily required) when the purpose of collection related to national security, defense, public security, criminal offenses, breaches of ethics

⁶ Further manipulation comprises all sorts of *private data* manipulations or uses for purposes that are not expressed when the *private data* was collected.

for regulated profession, financial interest of the E.U., for the protection of the data subject or of the rights and freedoms of others. {cf E.U. DPD Art. 13.}

1.2.3 Access to Rectify, Erase, or Block

Service providers should allow users to *access* their own *private data* challenge its correctness, and rectify, erase, or block it where appropriate. As shown in Fig. 1.6 the rectification cycle involves four processes: request, retrieval, challenge, and rectification/erasure/blocking processes. Where appropriate, any rectification/erasure/blocking related changes should be propagated to recipients.

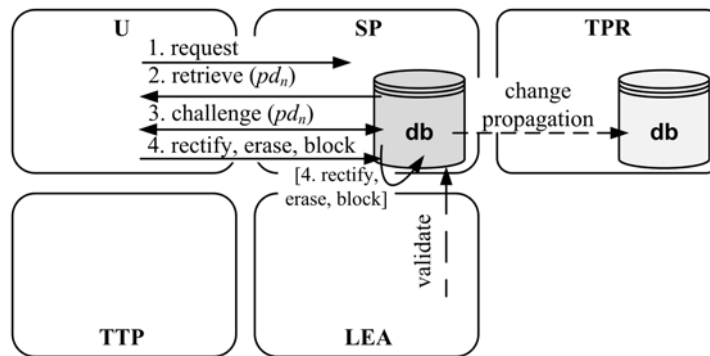


Fig. 1.6. Access related interactions

Access Requirements:

- **AR 1. Request:** A data subject should be allowed to query a service provider to know the presence of his/her *private data*.
 - **Exception 1:** The right to *access* his/her *private data* may be restricted (not allowed) when the stored *private data* is collected for national security, defense, public security, criminal offenses, breaches of ethics for regulated profession, financial interest of the E.U., for the protection of the data subject or of the rights and freedoms of others. {cf. E.U. DPD Art. 13.}
- **AR 2. Retrieval:** Service providers should respond within a reasonable time and for a reasonable charge (if existed). The response should explain the existence of the requested *private data*, (whether it has been used) how it has been used, and (if it is disclosed) with whom it has been shared. {cf. CFIPP 2, OECD 7, E.U. DPD Art. 12.}

- **AR 3. Challenge:** A data subject should be allowed to challenge the correctness of the retrieved *private data* related to him/her.
- **AR 4. Rectification, Erasure, or Blocking:** When the challenges are valid, the data subject should rectify, erase, or block the retrieved *private data*. {cf. CFIPP 4, OECD 7, MCPPI 9, E.U. DPD Art. 12.}
- **AR 5. Authentication and Authorization:** Before a user is allowed to *access* the database, either to rectify, erase, or block his/her *private data*, service providers should properly authenticate and authorize the user.
- **AR 6. Propagation of Rectification, Erasure, or Blocking:** To maintain data consistency, service providers should propagate the changes made by the data subject to their respective TPR. {cf. E.U. DPD Art. 12.}

1.2.4 Data Quality

Service providers should maintain the quality of *private data* they collected from their users. They need to maintain the reliability, relevancy, correctness, completeness, up-to-datedness, and adequateness of the collected *private data*. As shown in Fig. 1.7, where appropriate, any changes resulting from *data quality* manipulation should be propagated to TPR.

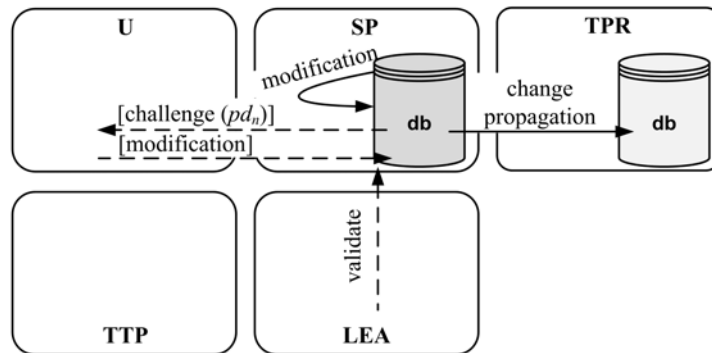


Fig. 1.7. Data quality related interactions

Data Quality Requirements:

- **DQR 1. Data Quality:** The quality of collected *private data* should be maintained. {cf. CFIPP 5, OECD 2, MCPPI 6, E.U. DPD Art. 6 and 12.}
- **DQR 2. Change Propagation:** To maintain data consistency, service providers should propagate any *data quality* related changes to their TPR. {cf. E.U. DPD Art. 12.}

1.2.5 Security

Service providers should take the appropriate technical and organizational measures to avoid unauthorized access, use, modification, or disclosure of their user's *private data* from their database. Their database should be readily available and designed to counter accidental destruction, loss, or alteration. Unless required by law, processing of *private data* should be confidential. Moreover, the integrity of collected *private data* should be preserved.

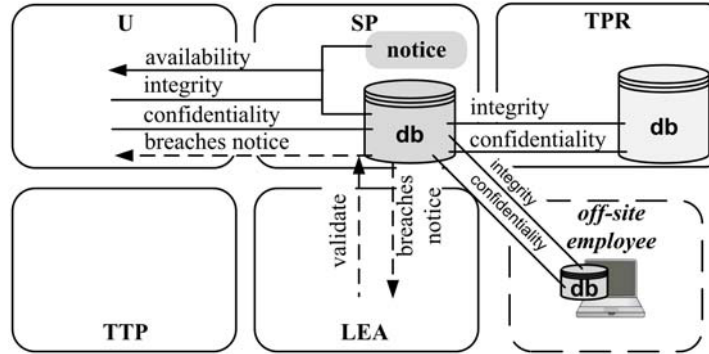


Fig. 1.8. Security related interactions

Security Requirements:

- **SR 1. Confidentiality:** The confidentiality of collected *private data* should be protected, to assure that the collected *private data* are shared with and used only by authorized entities. {cf. CFIPP 5, OECD 5, E.U. DPD Art. 16 and 17.}
- **SR 2. Integrity:** The integrity of user's collected *private data* and service provider's data practice *notice* statements should be preserved, when it is stored in the database and when it is in transit between users and service providers (or between service providers and recipients). {cf. CFIPP 5, OECD 5, E.U. DPD Art. 16 and 17.}
- **SR 3. Availability:** Service provider's databases should be readily available, to facilitate *private data access* and rectification processes. The service provider's data practice *notice* statement should also be readily available.
- **SR 4. Secure private data destruction:** When the retention period ends, user's *private data* should be destroyed securely.

1.2.6 Enforcement

An effective implementation of any of the above five generic *private data* protection requirements requires an *enforcement* and redress mechanism. Without *enforcement* and redress, these principles are plain guidelines and do not make a difference. In the past years, regulatory bodies around the world advocate two major alternative *enforcement* approaches, namely the industry self-regulation and the legislation driven *enforcement* approaches.

Industry self-regulation schemes are mainly built up with technical mechanisms in mind. In the self-regulatory schemes, compliance can be validated with membership of an industry association, with external audit verification for compliance, or with certification of the privacy policies (*see* Section 3.7). However, the approach has done very little to address the issue of redress, i.e. remedies and liabilities. Very often redress addressed through institutional mechanisms, such as correction of any misinformation or misdeeds, cessation of unfair practices, and rarely monetary compensation. In comparison with self-regulation, legislation based *enforcement* schemes efficient technical mechanisms that implement or validate legal compliances. However, legislative approaches thoroughly address extensive redress issues and define the conditions for liabilities and remedies. As a result, with a self-regulation approach, users are expected to resolve their *private data* related disputes either with the service provider itself, through a TTP, or through LEA. In legislation centric approaches, users are expected to resolve disputes through LEAs.

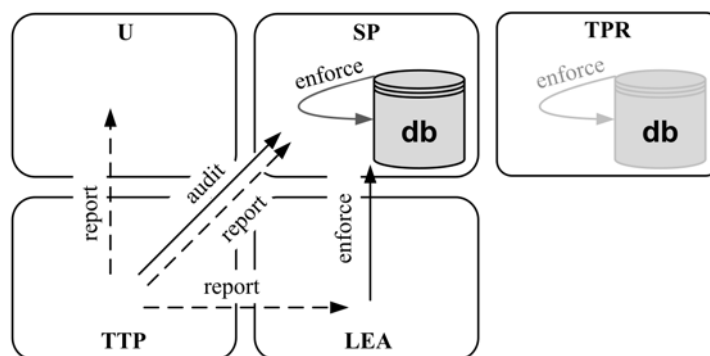


Fig. 1.9. Enforcement related interactions

As shown in Fig. 1.9, an *enforcement* should be carried out in three layers of protection. As a first layer of protection a service provider should employ internal privacy policy *enforcement* measures. Such internal *enforcement* schemes should validate whether user's privacy preferences and service provider's privacy policies are enforced as claimed. As a second layer of protection, the service provider's internal privacy policy *enforcement* practice (i.e. their ac-

tual data practice) should be compared and audited in relation to service provider's stated privacy policy *notice*. After such auditing by an independent TTP, any mismatch should be *publicly* reported for users and/or LEAs. Finally, LEA should validate the data practice of both service provider's and TTP s for legal compliance, as a third layer of protection.

Enforcement Requirement:

- **ER 1. Organizational Enforcement:** Service providers should employ internal privacy policy *enforcement* schemes to use user's *private data* w.r.t. user's privacy preferences and w.r.t. the service provider's privacy policy *notice* claims provided at the time of the *private data* collection. {cf. OECD 8, MCPPI 1, E.U. DPD Art. 22, 23, and 24.}
- **ER 2. Auditing and Reporting:** An independent TTP should audit the data practice of service providers and publicly report findings to users and LEAs.
- **ER 3. Compliance Enforcement:** The LEA should validate the data practice of the service provider and the independent TTP for legal compliance. {cf. E.U. DPD Art. 22, 23, and 24.}

Privacy Policy Languages

Privacy policy are a set of specification statements regarding the disclosure and use of user's *private data*. In literature, the term privacy policy often used to indicate two different contexts. In one context, the term privacy policy is used to express user's *private data* disclosure rules and it is often referred as user's privacy preference. For instance, using their privacy preferences (or policies) users can express which *private data* about them can be disclosed to whom and for what purpose. In another context, the term privacy policy is used to express the measures that service providers have take to use, manipulate, and/or further disclose the user's *private data* after data collection. Note that, privacy policies are not necessarily privacy friendly statements. In practice, both use's or service provider's privacy policies can contain privacy unfriendly statements and still be considered as privacy policies. For instance, a service provider's privacy policy claim can be read as "any member of our social-network can access all the personal details of other members." A privacy policy language defines a standardized syntax and semantics to create, communicate, and enforce user's privacy preferences and service provider's privacy policies. Nowadays, there are various alternative privacy policy languages in use and research. The major ones include P3P, APPEL, XACML, and EPAL. A brief survey of privacy policy languages is found in [16].

2.1 P3P

World Wide Web Consortium (W3C) developed P3P as a standard way for Web sites to expresses their privacy policies in a computer-readable format¹. Thus, P3P enabled Web browsers, such as Microsoft Internet Explorer, can retrieve and interpret the Web site's P3P policy file. The P3P 1.0 specification [5] defines an XML encoded policy language, that specifies the syntax and

¹ Traditionally Web sites express their privacy policies in a human-readable format.

semantics for creating and communicating Web site's privacy policy. The P3P policy language is explained further in Chapter 3.

2.2 XACML

XACML is a general policy language and an access control decision language of the *Advanced Open Standards for the Information Society* (OASIS). An XACML policy consists of six components:

1. **Rule:** a container for conditions and effect.
2. **Condition:** a boolean function over a subject, resource and environment attributes or any combination thereof.
3. **Effect:** intended consequence.
4. **Target:** subject, action, or resources the rule/policy intend to manipulate.
5. **Policy:** one or more rules.
6. **Obligation:** *Policy Enforcement Point* (PEP) action on either a permit or deny response.

An example policy in XACML syntax is included below to illustrate how the six different components can fit together. In the example, an accountant has a permit to print employee's payroll data between 8 AM and 5 PM.

```
<Rule Effect ="Permit">
  <Target>EmployeePayrollFile</Target>
  <Condition>
    <Apply FunctionId = "AND">
      Role = "Accountant",
      Action = "Print",
      Time >= 8am, Time <= 5pm
    </Apply>
  </Condition>
</Rule>
```

In 2005, "Privacy policy profile for XACML v2.0" [6] was approved as an OASIS standard and it defines two standard attributes.

1. *urn:oasis:names:tc:xacml:2.0:resource:purpose*: Specifies the purpose for which the *private data* is collected, i.e. this fulfills the *private data* collection transparency principles of the fair data practice principles (see Section 1.2).
2. *urn:oasis:names:tc:xacml:2.0:action:purpose*: Specifies the purpose for which access to the *private data* is requested. It indirectly address *private data* use limitation of the fair data practice principle (see Section 1.2).

Access control can be defined as a security mechanism that controls "who can accesses what, under what condition." If this definition is required to

incorporate privacy protection in the context of XACML, it can be redefined as “who can access what, under what condition and for what purpose.” The inclusion of the two attributes *fairly* makes XACML a privacy aware access control policy language.

2.3 EPAL

IBM’s EPAL is a formal language designed for writing enterprise privacy policies. It is an interoperability language for exchanging privacy policies between applications and an enterprise. Unlike P3P and other privacy policy languages EPAL aspires at specifying enterprise-internal privacy policies. So it does not define a global terminology as P3P. Preparing privacy policy with EPAL requires a good collection of vocabulary that formalizes enterprise specific privacy practices and a hierarchy of purposes for which the enterprise collects data. The syntax of EPAL vocabularies includes six major components:

1. **User categories:** classifying users as administrators, doctors, etc.
2. **Data categories:** classify data as customer data, student data, medical data, etc.
3. **Purposes:** state the purposes for which data is used or is going to be used.
4. **Actions:** perform certain operations on data resources like disclose, read, etc.
5. **Conditions:** specify conditions that needs to be fulfilled to access enterprise data resource.
6. **Obligations:** it is a step that needs to be taken by the enterprise because of legislation and privacy policy obligation, For example, “user’s search log data has to be deleted after two year”.

In the following EPAL policy the delivery department can access customer’s record, in this case Bob’s *private data*, for delivery processing purpose.

```
<epal-query>
  <user-category refid="DeliveryDepartment"/>
  <data-category refid="CustomerRecord"/>
  <purpose refid="DeliveryProcessing"/>
  <action refid="Store"/>
  <container refid="CustomerRecord">
    <attribute refid="CustomerID">
      <value>Bob</value>
    </attribute>
  </container>
</epal-query>
```

2.4 APPLE

APPEL is a W3C specification that aims at creating a standard language for expressing user privacy preferences. As the origin of P3P traced back to *Platform for Internet Content Selection* (PICS) (see Chapter 3), APPEL's rules specifications also originate from PICS Rules² [17].

P3P user agents may use APPEL rules for specifying user privacy preferences; however, user agents are free to use their own representation. If a P3P user agent uses APPEL, matching user's privacy preference with Web sites P3P policy is performed as follows. First, the user agent fetches the Web site P3P policy and passed it to APPEL engine as *evidence*. The APPEL engine uses an APPEL that file contains the user's privacy preferences as a serious of *rules*. Then, the APPEL engine matches the evidence against each rule and takes an appropriate action.

In the following APPEL preference policy, users will get a warning message if their *private data* is intended to be shared with adelivery service provider (i.e. with a TPR) in addition to the service provider.

```
<appel:RULE behavior="accept" prompt="yes"
description="Warning! Data may be shared with
delivery company">
  <p3p:POLICY>
    <p3p:STATEMENT>
      <p3p:RECIPIENT appel:connective="or" >
        <p3p:same/>
        <p3p:delivery/>
      </p3p:RECIPIENT>
    </p3p:STATEMENT>
  </p3p:POLICY>
</appel:RULE>
```

Further explanations of APPEL's syntax and semantics can be found inside the APPEL working draft documentation [8].

² In the PICS language, PICS Rules are used to specify user preferences on PICS labels.

P3P

The origin of P3P is traced back to the 1995 PICS [18] of the W3C. PICS uses a criterion named *rating system* for labeling Web content for children. It is mainly used for rating scales for sex, nudity, and violence contents. In 1996 Reidenberg demonstrates how PICS can be used for rating Web sites data practices [19]. Subsequently the idea of using PICS for privacy flourished and in 1997 P3P is officially launched as a W3C project [20].

3.1 Retrieving P3P Policy

Requesting and transmitting P3P policies on the Web is based on the standard *Hypertext Transfer Protocol* (HTTP) that Web browsers used to communicate with Web servers. In general, the complete interaction between P3P enabled Web browsers¹ and Web sites with P3P policy over HTTP is illustrated in Fig. 3.1.

As shown in Fig. 3.1 the negotiation starts with a request for the policy reference file. The policy reference file contains the path of the P3P policies, for each part (or page) of the Web site. A user agent then looks for the right P3P policy. When it finds the right P3P policy, it parses it and matches it with the user's privacy preferences. Whenever the user's privacy preference matches the Web site's P3P policy, a user can browse that Web site. In addition, every time a Web site sets cookies, special HTTP headers are used to transmit the P3P compact policy².

¹ P3P enabled Web browsers read Web site's P3P privacy policy and communicate it to the user. They also provide user agent implementation. Microsoft Internet Explorer is a P3P enabled Web browser.

² Compact policies are a shortened version of a full P3P policies that only describes Web site's privacy policy related to cookies (*see* Appendix B.2).

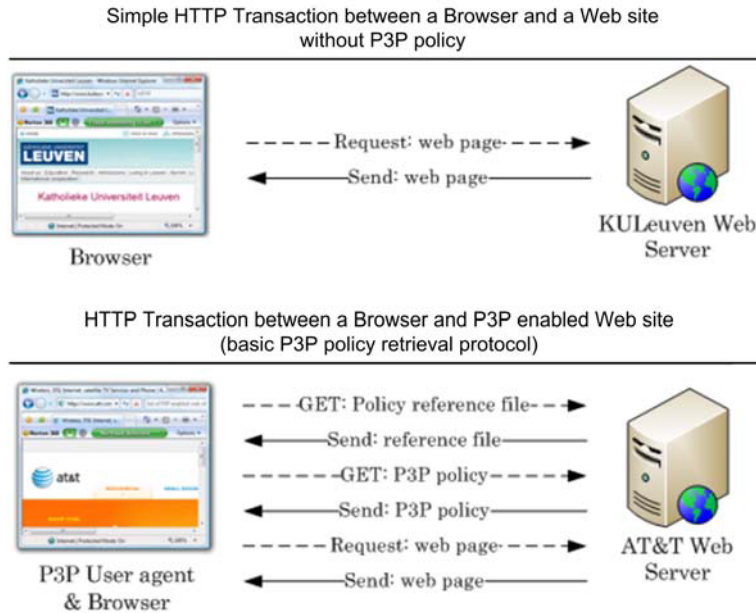


Fig. 3.1. Retrieving P3P policy

3.2 Elements of P3P Enabled Web Site

In addition to the main P3P policy file, a P3P enabled Web site incorporates the following compulsory and optional parts:

1. **Policy Reference File:** A P3P Policy reference file tells a user agent which P3P policy applies to which URL in a Web site. P3P enabled Web site needs to have at least one policy reference file.
2. **Data Schema:** Data schema is an optional component of a P3P enabled Web site. Web sites are required to include data schema files, if their policy introduce new data elements that are not included the P3P Basic Schema.
3. **Opt-In or Opt-Out Policy:** Opt-in and opt-out³ explains how users can apply opt-in or opt-out choices.
4. **P3P Header:** P3P header is an HTTP response header which tells the location (URL) of a P3P policy reference file. It may also include a compact policy.

³ Opt-in and opt-out in P3P lingo refer to user *consent* regarding the disclosure of their *private data*. Opt-in refers to a condition in which a user choose that their *private data* can be used for a particular purpose. On the contrary, opt-out refers to a situation where users request that their *private data* cannot be used for a particular purpose.

5. **P3P Policy File:** A P3P policy file in which organizations enumerate their privacy practices. P3P enabled Web sites need to have at list one P3P policy file. Appendix B.1 includes an example P3P policy file XML notation.
6. **Human-Readable Privacy Policy File (or Page):** Certain parts of P3P policy needs further explanations, such as DISPUTES, REMEDIES, and CONSEQUENCE elements. A human-readable policy file provides those explanations in a natural language. However, even if it conveys additional explanations, the human-readable policy must be consistent with its corresponding P3P policy file⁴.
7. **Compact Policy:** Compact policy is an optional component for a P3P enabled Web site. It is an abbreviated version of the full P3P policy designed to describe privacy practices related to cookies (*see* Appendix B.2).

3.3 P3P Policy File

As discussed in Section 3.2, a P3P policy consists of machine readable assertions of the Web site's privacy policy written in a standard privacy vocabulary. These assertions of a P3P policy can be classified into *general assertion* and *data-specific assertion*. General assertion state general declarations that apply generally to Web sites privacy practice. On the other hand, data-specific assertions state data-specific declaration related to Web sites practice in handling *private data*. The six general assertions are enumerated as follows:

1. **The POLICY element:** tells the location of human-readable policies and the opt-out policy.
2. **The TEST element:** is used to inform that the policy is written for testing purposes only. It is an optional tag and a policy that contains this tag should not be considered as a valid P3P policy (*see* Appendix B.1).
3. **The ENTITY element:** provides the Web site's contact information. In the P3P policy syntax this tag should contain the name of a legal entity (a person, business, or an organization that owns the Web site) and additional contact information (such as a phone number and postal address). {cf. CFIPP 1, E.U. DPD Art. 10, 11, and 19.}
4. **The ACCESS element:** explains whether a Web site allow users to *access* their *private data* collected by that particular Web site. If the Web site allows, the ACCESS element also explains which *private data* a user is allowed to *access*. {cf. CFIPP 2, OECD 7, MCPPI 9, E.U. DPD Art. 12.}
5. **The DISPUTES element:** explains what users can do if they have privacy related dispute with the Web site. It can be handled through contacting customer service of the Web site, by contacting privacy seal

⁴ Note that the human-readable privacy policy is different from the privacy summary report of Microsoft Internet Explorer 7 privacy policy viewer.

provider, or with a court where a user can file legal complaint. {cf. OECD 8, MCPPI 1, E.U. DPD Art. 22, 23, and 24.}

6. **The REMEDIES element:** explains the possible remedies offered by the Web site to users in case a policy breach occurs. {cf. E.U. DPD Art. 22.}

Data-specific assertion of a P3P policy file contains six P3P STATEMENT elements. The following is a short description:

1. **The CONSEQUENCE element:** contains a human-readable explanation why the requested *private data* is valuable in particular instance. For example, a typical consequence statement might read as follows “We offer a 15% discount and product catalogue for those joined our customer mailing list.”
2. **The NON-IDENTIFIABLE element:** is an optional tag that is only used if a Web site does not collect any identifiable data or anonymized the data it collects.
3. **The PURPOSE element:** describe purpose of the *private data* collection. {cf. OECD 3, MCPPI 2, E.U. DPD Art. 6, 18, and 19.}
4. **The RECIPIENT element:** clarify with whom the collected *private data* might be shared. {cf. E.U. DPD Art. 4 and 11.}
5. **The RETENTION element:** explain Web sites policy regarding *private data* retention practices. {cf. MCPPI 5, E.U. DPD Art. 6 [21].}
6. **The DATA element:** specifically tells which data a Web site is intend to collect. {cf. E.U. DPD Art. 19.}

The P3P vocabulary subjected by the P3P working group might not adequately express some Web sites privacy related practices. As a result, the P3P specification provide an EXTENSION element to let Web sites extend the syntax of the vocabulary of P3P. Refer to Appendix B.1 to understand how the general and data-specific assertions of P3P are represented in an XML policy file.

3.4 P3P User Agents

In P3P infrastructure, browser’s user agent is used to retrieve the Web site’s P3P policies, to interpret them, and carry put a given action according to the user’s privacy preferences. A user agent action can range from showing a simple informative message to blocking the requested Web site. In practice, informative user agent can use a picture icon, a text message, sound or any combination of the three. P3P user agents are also used to assist users in specifying their privacy preferences. A P3P compatible user agent might use an APPEL rule set to express user privacy preferences. However, a user agent can be P3P compliant without implementing a APPEL rule set.

In general P3P user agents can be classified into *informative-only* or *automatic* user agent. The former simply inform whether Web site's privacy policy matches with user privacy preferences or not. Automatic P3P user agent, on the other hand takes certain actions, such as blocking cookies or blocking access to certain Web sites. Some P3P agents are generic and offer little or no option for user to specify detailed privacy preference in comparison to other customizable P3P user agents.

It is possible to design P3P user agent in different ways, such as an agent built into Web browsers, as a standalone end user application, as Web browsers plug-ins or add-ons. It is also possible to design P3P user agents for personal computers, PIN-pad readers, cell phones and other similar devices.

3.5 Built-In P3P User Agents

P3P enabled Web browsers use their built-in user agent to interpret Web sites' P3P policies. Microsoft Internet Explorer (starting from version 6) is P3P enabled. As shown in Fig. 3.2 , the user agent included in Microsoft Internet Explorer 6 and 7 mainly designed to filter cookies.



Fig. 3.2. Internet Explorer 7, cookie filtering slider

Cookie filtering in Microsoft Internet Explorer uses compact P3P policies instead of the full P3P policy⁵. Based on the settings a user selects Microsoft

⁵ Consult Appendix B.1 and B.2 to understand the difference between full and compact P3P policy.

Internet Explorer accept, deny, downgrade, or leash cookies⁶. As shown in Fig. 3.3, every time a cookie is denied, downgraded, or leashed a small eye icon with the ‘not allowed’ sign appears on the status bar of Microsoft Internet Explorer. In addition to cookie filtering, Microsoft Internet Explorer provides a P3P policy viewer.



Fig. 3.3. Privacy icon in Microsoft Internet Explorer 7

In summary, Microsoft Internet Explorer has a built-in P3P user agent implementation focuses only on cookies. It falls short implement a full fledged user agent. As a result, users have a very limited ability to specify their privacy preferences using Microsoft Internet Explorer user agent.

3.6 Privacy Bird

AT&T’s Privacy Bird [22] is an informative-only P3P user agent that works as browser helper object for Internet Explorer. Privacy Bird includes a P3P policy evaluator engine that compares Web site’s privacy policy with user’s privacy preferences. The user privacy preference is encoded as an APPLE rule set.

As shown in Fig. 3.4, the Privacy Bird uses different bird icons to indicate whether the user’s privacy preferences matches with Web site’s P3P policy. The bird icon changes its color and shape according to the comparison result and also serves as a button to access Privacy Bird menu. A green bird indicates that the Web site’s P3P policy matches with the user’s privacy preferences. A red bird indicates that the Web site’s P3P policy conflicts with the user’s privacy preferences. A yellow bird appears when the Privacy Bird is unable to read the P3P policy of a given Web site. The Privacy Bird cannot read P3P policy when a Web site does not have a P3P policy, when the Web sites P3P policy contains error, or when the Web sites P3P policy has expired. A gray bird appears when the Privacy Bird has been disabled.

Privacy Finder [23] is an AT&T prototype that makes use of Privacy Bird evaluator engine to compare the user’s privacy preferences with the Web site’s P3P policies for search results. In comparison with other user agents, the Privacy Bird gives more control for users to specify their privacy preferences.

⁶ Downgrade cookies are deleted when they expire or the Browser session ends. Leasing cookies can only happen in first-party context and not in a third-party context.



Fig. 3.4. Privacy Bird indicator icons

3.7 Privacy Seals

The introduction of privacy seal is mainly intended to enable trust. In the current practice, seal providers makes sure that Web site's P3P policy matches with the actual Web site's data practices, before issuing a privacy seal [20]. In most instances, seal providers define minimal baseline requirements to issue their seals for service providers. In addition, for Web sites that follows the self-regulatory initiatives, seal providers play a major role as dispute handlers. The following is a part of an example P3P policy, in which a privacy seal provider serves as a dispute handler.

```

<DISPUTE-GROUP>
  <DISPUTE resolution-type = "independent"
    service="http://www.bbbonline.org"
    short-description="BBBOnline">
    <LONG-DESCRIPTION> BBBOnline Privacy Program
    </LONG-DESCRIPTION>
    <IMG src=
      "http://www.PizzaDC.be/privacy/image/privacyseal5.gif"
    Alt="BBOnline Privacy Seal"/>
  </DISPUTE>
  ...
</DISPUTE-GROUP >

```

The DISPUTE element of a P3P policy have four different resolution-types: customer service [*service*], independent organization [*independent*], court [*court*] and applicable law [*law*]. “Independent” attribute is used when a Web site wants to resolve privacy disputes with an independent organization, like a privacy seal provider.

Nowadays TRUSTe [24] and BBBOnline [25] are among the major privacy seal providers. They provide various customized privacy seals, such as general Web sites privacy seal, children Web sites privacy seal, eHealth Web sites privacy seal, E.U. Safe Harbor privacy seal, and so on. Fig. 3.5 shows a sample of TRUSTe and BBBOnline privacy seal icons.

The different icons from TRUSTe and BBBOnline mainly designed to address the sector centric self-regulation approach. For instance the TRUSTes eHealth seal is a clear example of sector specific privacy seal. On the 14th of July 2008, E.U. issued its first European Privacy Seal for *ICT products and*

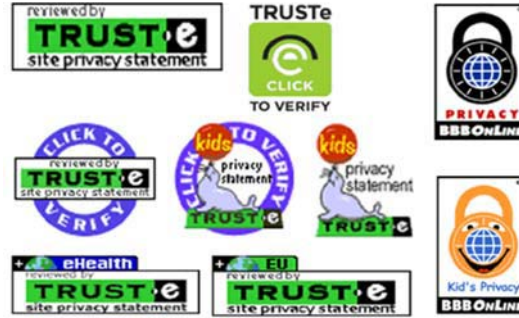


Fig. 3.5. TRUSTe and BBBOnline privacy seals

IT-based services for a search engine called ixquick⁷. The seal is issued for Web sites that comply with the E.U. DPD and security law through EuroPriSe. EuroPriSe is intended to improve consumer protection, civil rights and increase trust in IT in E.U. member states. Fig. 3.6 shows the EuroPriSe seal icon that is provided to ixquick search engine.



Fig. 3.6. The first E.U. [EuroPriSe] privacy seal for ixquick

⁷ <http://eu.ixquick.com/eng/>

Evaluating P3P

Based on the generic fair data practice requirements explained in Section 1.2, this Chapter evaluates the capabilities and limitations of P3P.

4.1 Capabilities

As shown in Table 4.3 and explained below, P3P is capable of addressing only the following *notice* and *consent* related requirements.

NR 3.1

Identification. The ENTITY element of P3P allows service providers to identify themselves to users.

NR 3.3.

Content. The DATA (DATA GROUP) element of P3P lets service providers present the list of the user's *private data* they intend to collect.

NR 3.4

Purpose. The PURPOSE element of P3P addresses eleven predefined purpose categories and leaves an optional extension to include other categories of purposes. Using this element service providers can specify the intended purpose of user's *private data* collection.

NR 3.5

Retention. The RETENTION element of P3P addresses four predefined retention categories. Using this element service providers can express for how long they intended to retain user's *private data*.

NR 3.6

Sharing. The RECIPIENT element of P3P includes six predefined recipient categories. Using this element a service provider can express with which third party recipient it intend to share user's *private data*.

NR 3.7

Access. Rectification, Erasure, or Blocking. Using P3P ACCESS element service providers can inform users whether users are allowed to *access* their own *private data* or not.

NR 3.9

Accountability. Accountability is fairly addressed by the DISPUTE and REMEDIES element of P3P

CR 1

priConsent. The P3P opt-in and opt-out policies can encode the service provider's *consent* rules.

4.2 Limitation

As shown in Table 4.3 and explained below, P3P falls short to address the following *notice*, *access*, *data quality*, *security*, and *enforcement* related requirements.

NR 1

Availability. The P3P specification provides four alternative mechanisms to indicate the location of a P3P policy reference file. A P3P policy reference file can be available in a predefined 'well-known' location (i.e. available on the Web site at the path "/w3c/p3p.xml"), through an HTML/XHTML link tag, or through an HTTP header [5]. Availability wise, the availability of a P3P policy and P3P policy reference files are dependent on the availability of the Web site itself.

NR 2

Assurance. As expressed in Section 3.7, a TTP can certify a P3P policy file with a privacy seal to attest its trustworthiness. Although, this attestation is not a part of the actual P3P protocol and it is optional. With the current practice it does not prove the correspondence between the actual data practice and published Web site's privacy *notice*.

NR 3.2

Collection. Except the CONSEQUENCE element that explains the consequences if data collection is accepted or denied by the user, P3P does not justify whether a given *private data* collection is lawful and fair. Moreover, P3P gives no exclusive collection *notice* concerning how the user's *private data* is going to be collected (such as passive or active data collection). It also does not specify whether a given data collection is mandatory or voluntary.

NR 3.6

Sharing.	The six sub classes of P3P RECIPIENT element are: ours, delivery, same, other-recipient, unrelated, and public [5]. However, Art. 6, 18, and 19 of the E.U. DPD strictly regulate E.U. citizen's <i>private data</i> sharing and its transfer to third countries. In the E.U. DPD context, P3P's RECIPIENT element is not adequate to express E.U. citizens <i>private data</i> sharing with third countries.
NR 3.8 Security.	A P3P <i>notice</i> has no element for service providers to communicate the <i>security</i> measures they have taken to safeguard user's <i>private data</i> . Thus, using P3P, users are not aware of to what extent the confidentiality of their <i>private data</i> is protected or to what extent the integrity of their <i>private data</i> is preserved.
CR2-2.1 <i>secConsent</i> .	After the user's <i>private data</i> has been collected, P3P can not be used to request user's <i>secConsent</i> .
AR 1-6 Access.	Access to Rectify, Erase, or Block. Besides giving a <i>notice</i> whether an <i>access</i> is allowed or not, P3P can not be used to actually <i>access</i> user's <i>private data</i> .
DQR 1-2 Data Quality.	P3P can not be used manage <i>data quality</i> related operations.
SR 1-6 Security.	The P3P policy provides neither a <i>notice</i> nor a <i>security</i> mechanism to preserve the <i>security</i> of user's <i>private data</i> . However, user's <i>private data</i> confidentiality, integrity, and availability, or secure <i>private data</i> destruction can be managed by existing <i>security</i> mechanisms.
ER 1-3 Enforcement.	Using P3P users can not verify the <i>enforcement</i> of their privacy preferences or service providers promises after their <i>private data</i> is being collected. P3P cannot be used to employ or validate internal organizational data practices. It cannot be used to audit or report service provider's data practices. It cannot also be used to validate compliance or enforce legal obligations.

Requirement	CFIPP	OECD	MCPPI	E.U. DPD	P3P	
Notice	NR 1	x	Openness	Art. 21	x	
	NR 2	x	x	x	x	
	NR 3.1	Principle 1	x	Art. 10, 11, & 19	Entity	
	NR 3.2	x	Collection limitation	Art. 6	Consequence	
	NR 3.3	x	x	Art. 19	Data	
	NR 3.4	Principle 2	Purpose specification	Identifying purpose	Art. 6, 18, & 19	Purpose
Consent	NR 3.5	x	x	Art. 6	Retention	
	NR 3.6	x	x	Art. 10, 11, 18, & 19	Recipient	
	NR 3.7	Principle 4 & 5	Collection limitation, individual participation	Accuracy, individual access	Art. 10 & 11	Access
	NR 3.8	Principle 5	Security safeguards	Safeguards	Art. 8	x
	NR 3.9	x	Accountability	Accountability	Art. 22, 23, & 24	Dispute, Remedies
	CR 1	x	Collection limitation	Consent	Art. 7, & 8	Opt-in, opt-out
Access	CR 2	Principle 3	Use limitation	Limiting use, disclosure, & retention	x	x
	CR 2.1	x	x	x	x	x
	AR 1	Principle 2	Individual participation	Individual access	Art. 12	x
	AR 2	x	Individual participation	Individual access	Art. 12	x
	AR 3	x	Individual participation	Individual access	Art. 12	x
	AR 4	x	Individual participation	Individual access	Art. 12	x
Data Quality	AR 5	x	x	x	x	x
	AR 6	x	x	Art. 12	x	x
	DQR 1	Principle 5	Data quality	Accuracy	Art. 6 & 12	x
	DQR 2	x	x	x	Art. 12	x
	SR 1	Principle 5	Security safeguards	x	Art. 16 & 17	x
	SR 2	Principle 6	Security safeguards	x	Art. 16 & 17	x
Enforcement	SR 3	Principle 7	Security safeguards	Individual access	Art. 12	x
	SR 4	x	x	x	x	x
	ER 1	Principle 5	Accountability	Accountability	Art. 22, 23, & 24	x
	ER 2	x	x	x	Art. 22, 23, & 24	x
Enforcement	ER 3	x	Challenge compliance	Challenge compliance	Art. 22, 23, & 24	x

Table 4.3. Summary on the capabilities and limitations of P3P

Key: x equals not applicable.

Concerns, Discussions, and Future Work

This Chapter briefly reflects on P3P related general concerns, overall privacy policy related interactions, and future work.

5.1 Concerns

P3P policies are only promises. There are no clear technical framework by far that actually enforces and/or audits the *enforcement* of user's privacy preferences or Web site's P3P policy promises. If there are no technical capabilities to prove a violation and make service providers accountable for their misdeeds, they are free to violate user's privacy preferences or even deny their own promises.

Applicability of P3P policies across transnational networks are very limited. For instance, the German privacy protection law is applicable only if the service provider has its headquarters or at least a subsidiary in Germany [26]. As a result, the applicability of P3P policies across trans-national networks and accountability of service providers are very different, ambiguous, and may potentially contradictory. Without a single universally agreeable *private data* protection law, the enforceability of P3P policy are very limited to an applicable law and national boundaries. Though, P3P policies are intended to be communicated in a global network without any boundary limitation. On one hand, it is very difficult for users to verify the applicability a P3P policy to their country privacy protection law. On the other hand, for service providers it is very difficult to tailor their P3P policies to make them applicable across trans-national networks and users across various nations¹.

¹ This concern might reach its climax in nations like the U.S. that have different privacy protection laws across states, even within the one nation. The E.U. DPD might also suffer from different interpretation (or adoption), different national privacy protection, and nation specific exceptions across E.U. member nations.

P3P lacks privacy policy enforceability across multiple domains. In the current P3P formulation, a user lacks control over his/her *private data* after the initial disclosure. Service providers also lack control over their user's *private data* after they share it with their recipients. Without a certain type of policy *chain-enforcement* across multiple domains, recipients are free to use the user's *private data* for unintended purpose. Moreover, P3P is inadequate for environments where multiple service providers are involved in collecting and managing *private data* such as federated identity management.

A P3P policy may be changed from time to time². For example, in the past when Amazon changes its privacy policy, customers were informed that Amazon will share their *private data* with third party business partners of Amazon. Although, Amazon's previous privacy policy has stated no intention of sharing its customer *private data* with TPR [27]. The challenge is once the new policy gets published; there is no technical protection that forbids Amazon from sharing its old customer *private data* which is collected before the policy change takes place. Moreover, P3P does not come up a feedback mechanism to inform users about the policy change. Therefore, with P3P it is possible to misuse already collected user's *private data*, as long as changing ones Web site's privacy policy is only a matter of posting a new one.

P3P empowers service providers. P3P can be used to deceive users to reveal their *private data* in exchange to Web site's services. The CONSEQUENCE elements of P3P can be used to deceive users with carefully crafted benefits, such as price discounts or free memberships. In such scenario, users with very restricted privacy preferences will have difficulties to access most Web sites.

5.2 Discussion

At the user side of the privacy policy landscape, users should be able to specify and communicate their privacy preferences and *private data access* claims to service providers. User should be able to fetch and analyze service provider's privacy policies. Therefore, at the user side, privacy-aware user agents, such as Privacy Bird or Internet Explorer built-in user agent, should be able to fetch *identification, collection, content, purpose, retention, sharing, access, security, and accountability* (NR 3) related *notices* of service providers. These user agents should be able to evaluate and/or verify the trustworthiness of service provider's privacy policy claims (NR 2). They should be able to communicate user's privacy preferences, *consents*, and *private data access* claims (CR 1, CR 2, and AR 1) to service providers. Where rectification/erasure/blocking is appropriate; user agents should also be able to facilitate *authentication* (AR 5), *private data retrieval*, (AR 2), *challenge* (AR 3), and *rectification* (AR 4) interactions between users and service providers. In this side of the privacy policy landscape, P3P plays no role.

² A P3P specification demands privacy policies to remain unchanged at least for 24 hours.

At the service providers side of the privacy landscape, service providers should be able to communicate their privacy policies to users. They should be able to retrieve user's privacy preferences, negotiate user's consents, and manage user's *private data* queries. They should be able to enforce user's privacy preferences. They should also be able to enforce their own privacy policy claims and comply with legal obligations. Therefore, at the service providers side, service providers should use privacy policy communication languages, such as P3P, to present their assurance attestation(NR 2) and their *collection, content, purpose, retention, sharing, access, security, and accountability* (NR 3) related claim statements to users.

They should employ privacy-aware identity management systems to negotiate the user's consent and fetch the user's *private data* together with the user's privacy preferences (CR 1 and CR 2). These identity management systems should facilitate the user's authentication (AR 5) and *private data* request negotiations (AR 1), where appropriate they should let users *access* (AR 2), challenge, (AR 3), and rectify/erase/block (AR 4) their own *private data*. Service providers should propagate any *data quality* (DQ 1 and 2) and/or rectification related (AR 6) changes to TPR s. These identity management systems should maintain the quality of collected user's *private data* (DQR 1) and also communicate the implemented safeguarding measures to protect user's *private data* (NR 3.8). Most importantly, service providers should use internal privacy policy enforcement languages, such as EPAL and XACML, to enforce their own privacy policy claims and also comply with legal obligations (ER 1). At the service providers side of the privacy policy landscape, P3P helps to communicate service provider's privacy polices; however it falls short to facilitate either the retrieval if user's privacy preferences or to adequately negotiate *secConsent*. P3P also fails to manage user's *private data access* requests, rectification/erasure/blocking processes, enforcing user's privacy preferences, or enforcing service provider's privacy policies.

At the TTP side of the privacy policy landscape, TTP should be able to evaluate the trust worthiness of service providers privacy policies and attest its correctness (NR 2). They should also be able to audit and report any irregularities of privacy policy *enforcement* (ER 2), user's participation (AR 1, AR 2, AR 3, AR 4, AR 5, and AR 6), *data quality* (DQ 1 and DQ 2), and *security* (SR 1, SR 2, SR 3, and SR 4), related practices to LEA. LEA in turn should be able to validate the data practices of service providers and TTP s for regulatory compliances (ER 3). Therefore, as shown far, in the overall privacy policy landscape, P3P plays only a very basic role.

5.3 Future Work

An effective deployment of P3P can be attained in two ways; one is through extending the current P3P policy language. Another one is through integrating P3P with other privacy policy languages, such as APPEL, EPAL, and

XACML, and related security and privacy schemes. With this in mind, future works on P3P are broadly classified into the following extensions and integration aspects.

- Extend or integrate P3P with other policy enforcement languages to make sure that the proper *enforcement* and *enforcement validations* of user's privacy preferences, service provider's privacy policies, and regulatory compliances are possible.
- Extend or integrate P3P with other policy and configuration languages to maximize the versatility of P3P, hence it can work contextually across trans-national networks (i.e. different nations) with different regulatory requirements.
- Extend or integrate P3P with other policy and *access* control policy languages to effectively manage policy changes both at the user's and service provider's side.
- Extend or integrate P3P with other security and privacy policy languages to adequately address *consent*, *access*, *data quality*, and *security* related requirements.
- Extend P3P to maximize its privacy policy *notice* coverage, meaningfulness, and context awareness³.

Apart from extending and integrating P3P, future work should be finding out ways to measure and attest the trust worthiness of P3P policy claims through real time auditing, matching, and reporting of service providers actual data practice versus their published *notices*. Also future work can apply our comprehensive yet generic requirements to find out the capabilities and limitations of other privacy policy related schemes or languages.

³ A context aware P3P policy *notice* can provide domain specific claim statements particularly tailored for certain domains or regions.

A

Fair Data Practice Principles

A.1 OECD Guidelines

1. Collection Limitation Principle: “There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.”
2. Data Quality Principle: “Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.”
3. Purpose Specification Principle: “The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”
4. Use Limitation Principle: “Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.”
5. Security Safeguards Principle: “Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data”
6. Openness Principle: “There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller “
7. Individual Participation Principle: “An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that

is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended”

8. Accountability Principle: “A data controller should be accountable for complying with measures which give effect to the principles stated above.”

A.2 Canadian MCPPI

1. Accountability: “An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organizations compliance with the following principles.”
2. Identifying Purposes: “The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.”
3. Consent: “The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.”
4. Limiting Collection: “The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.”
5. Limiting Use, Disclosure, and Retention: “Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.”
6. Accuracy: “Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.”
7. Safeguards: “Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.” Openness: “An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.”
8. Individual Access: “Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.”
9. Challenging Compliance: “An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organizations compliance.”

A.3 U.S. and E.U. Safe Harbor Principles

1. Notice: “Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.”
2. Choice: “Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.”
3. Onward Transfer (Transfers to Third Parties): “To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent(1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.”
4. Access: “Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or where the rights of persons other than the individual would be violated.”
5. Security: “Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.”
6. Data integrity: “Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.”
7. Enforcement: “In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual’s complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems

arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.”

B

P3P Examples

B.1 Example P3P Policy

```
<?xml version="1.0" encoding="UTF-8"?>
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">

  <!-- Expiry information for this policy -->
  <EXPIRY max-age='86400' />

  <!-- Custom data elements defined by this policy. -->
  <DATASHEMA>
    <DATA-DEF name='newdataset' short-description=
      'New Data Set'>
    </DATA-DEF>
  </DATASHEMA>

  <POLICY
    name='privacypolicy'
    discuri="http://www.pizzadc.be/privacypolicy"
    opturi="http://www.pizzadc.be/opt-out"
    xml:lang="en">

  <!-- Test-only policy - not for actual use -->
  <TEST/>

  <!-- Description of the entity making this
    policy statement. -->
  <ENTITY>
  <DATA-GROUP>
    <DATA ref="#business.name">Pizza Delivery
      Centre</DATA>
    <DATA ref="#business.contact-info.online.email">
```

```

        info@pizzadc.be</DATA>
<DATA ref="#business.contact-info.online.uri">
    http://www.pizzadc.be</DATA>
<DATA ref="#business.contact-info.telecom.
    telephone.number">0032 000 000 000</DATA>
<DATA ref="#business.contact-info.postal.
    organization">Pizza D.C.</DATA>
<DATA ref="#business.contact-info.postal.street">
    Geldenaaksebaan 00</DATA>
<DATA ref="#business.contact-info.postal.city">
    Heverle</DATA>
<DATA ref="#business.contact-info.postal.stateprov">
    Vlaams-Brabant</DATA>
<DATA ref="#business.contact-info.postal.postalcode">
    3000</DATA>
<DATA ref="#business.contact-info.postal.country">
    Belgium</DATA>
</DATA-GROUP>
</ENTITY>

<!-- Disclosure -->
<ACCESS><ident-contact/></ACCESS>

<!-- Disputes -->
<DISPUTES-GROUP>
<DISPUTES resolution-type="independent"
    service="http://www.beppc.be"
    verification="http://www.beppc.be/privacy/verify"
    short-description="bePPC">
    <LONG-DESCRIPTION>Belgium Privacy Protection
        Commission</LONG-DESCRIPTION>
    <IMG src="http://www.beppc.be/privacy/image/
        privacyseal16.gif" alt="bePPC privacy seal"/>
    <REMEDIES><correct/></REMEDIES>
</DISPUTES>
</DISPUTES-GROUP>

<!-- Statement for group "Customer Name" -->
<STATEMENT>
<EXTENSION optional="yes">
<GROUP-INFO xmlns=
    "http://www.software.ibm.com/P3P/editor/
    extension-1.0.html" name="Customer Name"/>
</EXTENSION>

```

```

<!-- Consequence -->
  <CONSEQUENCE>
    We collect your name to processes your order
    and delivery. Plus we offer a 10% discount
    for our online customers.
  </CONSEQUENCE>

<!-- Use (purpose) -->
  <PURPOSE><contact/></PURPOSE>

<!-- Recipients -->
  <RECIPIENT><ours/><delivery/></RECIPIENT>

<!-- Retention -->
  <RETENTION><indefinitely/></RETENTION>

<!-- Base dataschema elements. -->
  <DATA-GROUP>
    <DATA ref="#user.name.given"/>
    <DATA ref="#user.name.family"/>
  </DATA-GROUP>
</STATEMENT>

<!-- Statement for group "Customer Address" -->
  <STATEMENT>
    <EXTENSION optional="yes">
      <GROUP-INFO xmlns=
        "http://www.software.ibm.com/P3P/editor/
        extension-1.0.html" name="Customer Address"/>
    </EXTENSION>

<!-- Consequence -->
  <CONSEQUENCE>
    We collect your address to processes your order
    and delivery. Plus we offer a 10% discount for
    our online customers.
  </CONSEQUENCE>

<!-- Use (purpose) -->
  <PURPOSE><contact/></PURPOSE>

<!-- Recipients -->
  <RECIPIENT><ours/><delivery/></RECIPIENT>

<!-- Retention -->

```

```

<RETENTION><indefinitely/></RETENTION>

<!-- Base dataschema elements. -->
<DATA-GROUP>
  <DATA ref="#user.home-info.postal.street"/>
  <DATA ref="#user.home-info.postal.postalcode"/>
  <DATA ref="#user.home-info.postal.city"/>
</DATA-GROUP>
</STATEMENT>

<!-- Statement for group "Dynamic Data" -->
<STATEMENT>
  <EXTENSION optional="yes">
  <GROUP-INFO xmlns=
    "http://www.software.ibm.com/P3P/editor/
    extension-1.0.html" name="Dynamic Data"/>
  </EXTENSION>

<!-- No consequence specified -->

<!-- Use (purpose) -->
<PURPOSE><admin/><current/><develop/>
  <tailoring/></PURPOSE>

<!-- Recipients -->
<RECIPIENT><ours/></RECIPIENT>

<!-- Retention -->
<RETENTION><indefinitely/></RETENTION>

<!-- Base dataschema elements. -->
<DATA-GROUP>
  <DATA ref="#dynamic.clickstream.clientip.fullip"/>
  <DATA ref="#dynamic.cookies"><CATEGORIES>
    <computer/><financial/> <interactive/>
    <navigation/><online/><physical/>
    <preference/><purchase/><uniqueid/>
  </CATEGORIES></DATA>
</DATA-GROUP>
</STATEMENT>

<!-- End of policy -->
</POLICY>
</POLICIES>

```

B.2 Example P3P Compact Policy

CP= “IDC DSP COR CURa ADMa DEVa TAIa CONa OUR DELa IND
PHY ONL UNI PUR FIN COM NAV INT DEM PRE TST”

This compact policy is a shortened version of the P3P policy explained in Appendix B.1. Table B.1 explains the meaning of the acronyms used in the compact policy.

IDC	Access is available to contact information.
DSP	The policy contains at least one dispute-resolution mechanism.
COR	Violations of this policy will be corrected.
CURa	The data is used for completion of the current activity.
ADMa	The data is used for site administration.
DEVa	The data is used for research and development.
TAIa	The data is used for tailoring the site.
CONa	The data is used for contacting the user.
OUR	The data is given to ourselves and our agents.
DELa	The data is given to delivery services.
IND	The data will be kept indefinitely.
PHY	Physical contact information is collected.
ONL	Online contact information is collected.
UNI	Unique identifiers are collected.
PUR	Purchase information is collected.
FIN	Financial information is collected.
COM	Computer information is collected.
NAV	Navigation and clickstream data is collected.
INT	Interactive data is collected.
DEM	Demographic and socioeconomic data is collected.
PRE	Preference information is collected.
TST	Policy is for test purposes only.

Table B.1. The description of the acronyms in the compact policy

References

1. U.S. Department of Health, Education, and Welfare (1973) *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems.
2. Organization for Economic Co-operation and Development (1980) OECD, *OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*.
3. Che M, Grellmann W, Seidler S (1995) *Model Code for the Protection of Personal Information (CAN/CSA -Q830-96)*.
4. European Union (1995) Directive 95/46/EC of the European Parliament and of the Pouncil of 24 October 1995 *on the Protection of Individuals with Regard to the Rrocessing of Personal Data and on the Free Movement of such data*, Official Journal of the European Communities L 281.
5. L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle (2002) *The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification*, World Wide Web Consortium Recommendation.
6. T. Moses (2005) *Privacy Policy Profile of XACML v2.0: OASIS Standard*.
7. P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter (2003) *Enterprise Privacy Authorization Language (EPAL 1.2)*.
8. M. Langheinrich (1998) *A P3P Preference Exchange Language (APPEL)*, working draft.
9. United Nations (1990) A/RES/45/95, *Guidelines for the Regulation of Computerized Personal Data Files*.
10. Privacy Working Group, Information Policy Committee, and Information Infrastructure Task Force (1995) *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*.
11. APEC (2005) *APEC Privacy Framework*.
12. Privacy Commissioner (2006) *Australian National Privacy Principles*.
13. U.S. Department of Commerce (1995) *Privacy and the NII, Safeguarding Telecommunications Related Personal Information*.
14. Asia-Pacific Economic Cooperation (APEC) (2005) *Privacy Framework*.
15. Export.gov (2000) *Safe Harbor Framework*.
16. P. Kumaraguru, L. Cranor, J. Lobo, and S. Calo (2007) *A Survey of Privacy Policy Languages*. Proceedings of the 3rd Symposium on Usable Privacy and Security.

17. C. Evans, C. Feather, A. Hopmann, M. Presler, and P. Resnick (1997) *PICS Rules 1.1, W3C Recommendation*.
18. P. Resnick and J. Miller(1996) *PICS: Internet Access Controls without Censorship*, Communications of the ACM, vol. 39(10).
19. J. Reidenberg (1997) *Information Policy Rules through Law and Technology*, Proceedings of the 19th International Conference of Data Protection Commissioners.
20. L. Cranor(2002) *Web Privacy with P3P*, OReilly & Associates.
21. European Union (2006) Directive 2006/24/EC, *on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*.
22. Privacy Bird <http://www.privacybird.org/>
23. Privacy Finder, <http://www.privacyfinder.org/>
24. TRUSTe, <http://www.truste.org/>
25. BBBOnline, <http://www.bbb.org/online/>
26. R. Grimm and A. Rossnagel (2000) *Can P3P Help to Protect Privacy Worldwide?* Proceedings of the 2000 ACM workshops on Multimedia.
27. R. Hunter (2002) *World without Secrets: Business, Crime and Privacy in the Age of Ubiquitous Computing*, John Wiley & Sons, Inc.