P3P

Platform for Privacy Preferences

Seminar von Johannes Herlitz (j_herlit@informatik.uni-kl.de)

Das internationale World Wide Web Consortium (W3C) hat im April 2000 mit *P3P* ein neues auf HTTP aufsetzendes Protokoll für bessere Transparenz beim Surfen vorgestellt. Es beinhaltet ein maschinenlesbares Vokabular zur Beschreibung von Vorgehensweisen zum Schutz persönlicher Informationen, die beim Besuchen einer Web-Seite entstehen. Sowie das dazugehörige Protokoll zum Austausch dieser Informationen zwischen Browser und Web-Server. Statt seitenweise Kleingedrucktes zu lesen soll der Browser – einmal konfiguriert – die Aufgabe der Bewertung von Web-Seiten selbst übernehmen, um akzeptable von inakzeptablen unterscheiden ohne sich um juristische Feinheiten kümmern zu müssen.
Hier wird sowohl ein Überblick über das Prinzip als auch die Einblicke in die Syntax gegeben und einzelne Sprachelemente von P3P anhand von Beispielen erläutert.

1. Überblick

1.1. Problematik:

Beim Surfen im WWW gibt man, teils ohne es zu wissen, Informationen über sich preis, die vom Web-Server gespeichert und anschließend vom Anbieter dieser Seite auch für eigene Zwecke verwendet werden können. Klar ist, daß z.B. Name und Adresse in einem Online Adressbuch von Anbietern wie web.de gespeichert werden. Stellenweise wird aber auch ausgewertet, welchen Weg man durch den Internet-Dschungel wählt oder wie lange man irgendwo verweilt. Dies sind persönliche Informationen, an deren Schutz man normalerweise wohl nicht sofort denkt.

Eine kontinuierliche Nachfrage nach Anonymizer-Werkzeugen, wie zum Beispiel Anonymizer.com oder die "Freedom"-Software von Zero-Knowledge [1] zeigen, daß Nutzer des WWW sich Gedanken darüber machen, was Betreiber von Web-Seiten mit Ihren persönlichen Daten machen. Sie geben persönliche Informationen im Netz preis und haben keine Kontrolle darüber, was der Webseiten-Anbieter damit macht, z.B. ob er Sie an Dritte zu Marketingzwecken weitergibt.

Ganz ohne Preisgabe wenigstens einiger persönlicher Daten geht es anscheinend nicht, wenn man z.B. personalisierte Online-Terminkalender und Adreßbücher betrachtet; diese Eingaben ganz wegzulassen ist schwer möglich. An Online-Shopping ist natürlich ohne eine Postadresse gar nicht erst zu denken.

Wenn sich dann sogar einmal der vorsichtige Nutzer entschließt, ein Webformular auszufüllen, wäre es für ihn doch interessant, welche Wege seine Daten nehmen, wo sie schließlich überall gespeichert werden und wie die Firmen, die die Daten gespeichert haben, sie einsetzen. Außerdem könnte ihn interessieren, ob er seine Angaben im Nachhinein noch ändern oder sogar löschen kann.

Wie kann man den Nutzern von Online-Diensten also mehr Kontrolle und Überblick über ihre eigenen Daten geben ?

1.2. Ist-Zustand:

Zur Zeit ist es so, daß man sich beim Online-Shopping nach dem Aussuchen der Artikel, wenn man zum eher lästigen Teil der Bestellung, dem Angeben seiner Adresse, Bankverbindung, etc. übergeht, fast endlos durch AGBs, Verträge, etc. klickt, bevor man endlich den Kaufvertrag abschließen kann. Das Durchlesen von langen und komplexen juristischen Vertragsbestimmungen ist genauso unangenehm wie die ständige Kontrolle auf Veränderungen innerhalb der Vereinbarungen des Dienstleisters, wenn man öfter ein und denselben Dienst nutzt.

Lästig deswegen, weil man ja eigentlich seine Postanschrift, Kreditkartennummer, Telefonnummer, usw. einmalig in seinem Browser einstellen könnte und dieser könnte dann beim Abschluß der Bestellung in einem Online-Shop die Daten automatisch übermitteln. Läßt man dies aber ohne weitere Sicherheitsvorkehrungen zu, dann könnte sich natürlich jede beliebige Web-Seite Kreditkarten- oder Telefonnummer besorgen.

Betrachtet man Online-Shopping, können natürlich auch nicht erst beim eigentlichen Vertragsabschluß (der verbindlichen Bestellung) Informationen gesammelt werden, sondern auch schon vorher bei der Auswahl der Artikel: man verfolgt wann der Nutzer auf welchen Link klickt und kann so erstens feststellen, welchen Weg er durch die Site genommen hat und zweitens welche Web-Seite er wie lange betrachtet hat. Das Ergebnis dieser Datenaggregation nennt man einen "Clickstream".

So sammelt z.B. die Suchmaschine AltaVista [2] Informationen darüber, was man sucht und auf welche Links man klickt und schickt diese Informationen an das auf Internetwerbung spezialisiertes Unternehmen DoubleClick [3]. Wie man im Quellcode der Startseite von AltaVista sehen kann, befinden sich dort Verweise auf Dateien von DoubleClick. DoubleClick kann über Session-IDs ein Profil von einem Web-Nutzer ermitteln und feststellen wie lange er sich welche Web-Seite angeschaut hat, von welcher anderen Seite aus der Einstiegspunkt zur aktuellen Seite war und wo der Nutzer die Seite wieder verlassen hat. Zwar sind diese Datensätze dann noch ohne Namen oder Anschrift, aber die Speicherung der IP ist z.B. leicht möglich. DoubleClick kann dann entscheiden welche Art Werbebanner der Kunde eingeblendet bekommt und so gezielt an diesen Kunden-Typ Werbung übermitteln.

Zur Zeit wird DoubleClick anscheinend sogar wegen dieser Sache verklagt werden: "US-Gericht stimmt Sammelklage gegen DoubleClick zu" heißt es im Heise Newsticker [4].

Hier setzt P3P (Platform for Privacy Preferences) an: es überwacht, *wer wozu was* sammelt und evtl. an *wen was* weitergegeben wird.

1.3. Soll-Zustand:

Um das Problem zu lösen und die Privatsphäre zu gewährleisten, ist sowohl auf der technischen Seite eine Implementierung nötig, als auch auf der juristischen Seite eine darauf ausgerichtete Gesetzgebung und Strafverfolgung, mindestens innerhalb eines Landes. Wären entsprechende Paragraphen in den deutschen Gesetzen vorhanden, könnte schon jetzt P3P (Platform for Privacy Preferences) voll zur Geltung kommen und z.B. die Qualität deutscher Online Shops im Vergleich zu anderen steigern, vorausgesetzt, P3P wird von den Betreibern genutzt.

Wünschenswert ist eine weltweit vereinheitlichte Vorgehensweise bei der Benutzung, Speicherung und Weitergabe persönlicher Daten. P3P versucht dies im einfachsten Fall durch ein standardisiertes Set an leicht verständlichen Multiple-Choice-Fragen für den Webseiten-Betreiber, aus denen dann Policy Generatoren (z.B. das Java Programm "IBM P3P Policy Editor" [5] oder online durch den "PrivacyBot" [6]) die P3P-Dateien erstellen. Ein Nutzer stellt dann im Browser ein, wann er oder sie gewarnt werden will; dies geschieht dann beispielsweise durch ein Pop-Up-Fenster.

1.4. Eigenschaften von P3P (Platform for Privacy Preferences):

P3P ist ein XML-Protokoll, das auf HTTP aufsetzt. Ein Browser, der P3P unterstützt, überprüft, ob auf dem Web-Server bestimmte Dateien existieren und überträgt sie zum lokalen Rechner. Nach deren Interpretation entscheidet dann der Browser anhand der vom Benutzer eingestellten P3P-Optionen, ob die eigentlich anzuzeigende Seite für den Benutzer akzeptabel ist oder nicht.
Das P3P-Protokoll kann in verschiedenen Phasen, z.B. beim Online-Shopping während des Aussuchens von Waren oder beim Verlassen des Online Shops verwendet werden. Bei der Auswahl der Artikel wird ein sogenannter "Clickstream" gesammelt, die Information darüber, welche Seite man sich wie lange angeschaut hat. P3P kann modellieren, daß der Betreiber Clickstreams sammelt und man könnte auf Benutzerseite einstellen daß man schon dann gewarnt werden will, wenn eine Seite nur Clickstreams sammelt.

Man kann die Fähigkeiten von P3P grob in fünf Punkte für Vorgehensweisen nach außen und vier Punkte für Site-interne Politik einteilen.

Einstellungen nach außen (Datenfluß zur Site oder davon weg):

- *Wer* sammelt Daten ?
  Firma mit Name, Postanschrift, E-Mail Adresse, Telefonnummer kann in P3P Notation gespeichert werden (siehe 2.2.)

- *Was* genau wird gesammelt ?
  Datum, Name, Telefonnummer, Postanschrift, Online Adresse, IP-Adresse, Browserinformationen, Firmendaten, dynamische Daten wie cookies oder Mausklicks (siehe 2.3.)

- *Warum* wird meine Information gebraucht ?
  Braucht die Seite meine Information nur für die aktuelle Transaktion, um die Web-Seiten zu verbessern oder um Werbung gezielter einsetzen zu können ? (siehe 2.4.)

- Welcher Teil meiner Informationen wird *weitergegeben* ?
  Teilmenge von "*Was* wird gesammelt ?" (siehe 2.3. und 2.5.)

- *An wen* wird meine Information weitergegeben ?
  (siehe 2.5.)

Site-intern (Fragen, die nur die aufgerufene Seite allein betreffen):

- Kann ich im Nachhinein *ändern*, wie meine Daten benutzt werden ?
- Wie werden *Konflikte* und Zweifelsfälle gelöst ?
  (siehe 2.6.)
- Wie ist die Vorgehensweise (Policy) für die *Speicherung* meiner Daten ?
- Wo kann ich Details in vernünftiger, *verständlicher Form* nachlesen ?
  (siehe 2.7.)

1.5. Beispielszenario:

Trixi entscheidet sich bei einem Onlineshop "Beispielshop" unter `http://www.beispielshop.de/` vorbeizuschauen. "Beispielshop" hat P3P Policies auf allen Web-Seiten und Trixi benutzt einen P3P unterstützenden Web-Browser.

Trixi tippt die Adresse für Beispielshop in ihren Web-Browser. Ihr Browser kann automatisch die P3P Policy für diese Seite runterladen. Die Policy besagt daß die einzigen Daten, die durch die Seite gesammelt werden, die sind, die in den Zugriffsprotokollen des Web-Servers stehen. Jetzt vergleicht Trixies Web-Browser die heruntergeladenen Policies mit denen, die Trixi vorher eingestellt hat. Ist die Policy akzeptabel oder sollte Trixi kurz benachrichtigt werden ? Die Policies für diese Web-Seite seien jetzt einmal als für Trixi akzeptabel angenommen. In diesem Fall wird die Seite ganz normal ohne Pop-Ups dargestellt. Eventuell erscheint ein kleines Icon irgendwo in einer Leiste des Browsers um Trixi anzuzeigen, daß eine P3P Policy auf der Seite ist und diese mit ihren Einstellungen übereinstimmen.

Als nächstes klickt Trixi auf einen Link zum Online-Katalog der Seite. Der Katalog-Teil der Web-Seite hat etwas komplexere Software, welche Cookies benutzt, um einen Einkaufswagen zu realisieren. Da in diesen Bereichen der Seite mehr Informationen gesammelt werden, hat der Web-Server eine eigene P3P Policy um diesen Bereich abzudecken.

Wir wollen noch einmal annehmen, daß diese Policies mit Trixies Einstellungen übereinstimmen. Es werden also keine Pop-Up-Nachrichten in Ihrem Browser dargestellt. Trixi wählt ein paar Dinge zum Kauf aus und will dann die Bestellung aufgeben. Dazu muß Trixi noch ein paar zusätzliche Informationen angeben: Name, Adresse, Kreditkartennummer und Telefonnummer. Für diese Seite gibt es wieder eine neue P3P Policy, die beschreibt welche Daten hier gesammelt werden und versichert, daß diese Daten nur hier für die aktuelle Transaktion verwendet werden.

Trixi's Browser analysiert die P3P-Policy. Angenommen, Trixi hat in ihrem Browser eingestellt, daß sie immer dann gewarnt werden will, wenn jemand nach ihrer Telefonnummer fragt. In diesem Fall wird ihr Browser ein Pop-Up anzeigen, das Trixi informiert, daß die Web-Seite nach ihrer Telefonnummer fragt und zu welchem Zweck die Nummer gebraucht wird. Sie kann dann entscheiden ob dies akzeptierbar ist. Falls ja, kann sie mit der Bestellung weitermachen, im anderen Fall kann sie die Bestellung abbrechen.

Alternativ hätte Trixi in Ihrem Browser einstellen können, daß sie nur dann gewarnt werden will wenn jemand z.B. nach ihrer Telefonnummer fragt und sie an Dritte weitergibt oder die Nummer für mehr als die aktuelle Transaktion benutzt wird. In diesem Fall hätte sie bei obigem Beispiel keine Eingabeaufforderungen von Ihrem Browser erhalten.

2. P3P in Aktion

2.1.1. Serverseite

Das W3C gibt drei Methoden vor, um P3P zu aktivieren. Dazu muß ein sogenanntes "policy reference file" im XML Format gefunden werden. Die erste und vom W3C empfohlene Methode, diese Datei zu finden, ist, sie an einer vordefinierten Stelle zu speichern, der sogenannten "well-known location": `/w3c/p3p.xml`. Darin steht dann, für welche Bereiche vom Web-Server welche policy files gültig sind, z.B. Policy1.xml für die gesamte Seite ausser für alles unter /catalog/, /cgi-bin/ und /servlet/. Für /catalog/ soll stattdessen Policy2.xml gelten und für die anderen beiden unter Ausschluss von /servlet/unknown Policy3.xml. Beispiel 1 zeigt ein policy reference file für dieses Szenario.

```
<META xmlns="http://www.w3.org/2000/12/P3Pv1">
  <POLICY-REFERENCES>
    <POLICY-REF about="/P3P/Policy1.xml">
      <INCLUDE>/*</INCLUDE>
      <EXCLUDE>/catalog/*</EXCLUDE>
      <EXCLUDE>/cgi-bin/*</EXCLUDE>
      <EXCLUDE>/servlet/*</EXCLUDE>
    </POLICY-REF>
    <POLICY-REF about="/P3P/Policy2.xml">
      <INCLUDE>/catalog/*</INCLUDE>
    </POLICY-REF>
    <POLICY-REF about="/P3P/Policy3.xml">
      <INCLUDE>/cgi-bin/*</INCLUDE>
      <INCLUDE>/servlet/*</INCLUDE>
      <EXCLUDE>/servlet/unknown</EXCLUDE>
    </POLICY-REF>
  </POLICY-REFERENCES>
</META>
```

Beispiel 1: policy reference file

Die zweite Möglichkeit für den Browser, diese Datei zu finden, ist es, ihre Position serverseitig durch HTTP header anzugeben. Dazu muß man den Web-Server umkonfigurieren. Er muß eine zusätzliche Antwort-Zeile auf eine Client-Anfrage schicken. Beispiel 2 zeigt die drei Zeilen die in der Konfigurationsdatei eines Apache Web-Servers einzufügen sind um die Position auf /w3c/p3p.xml festzulegen.

```
<Location / >
  Header append P3P "policyref=\"http://foo.bar/w3c/p3p.xml \""
</Location>
```

Beispiel 2: Apache Web-Server Konfiguration

Die Dritte Möglichkeit ist, in HTML Seiten selbst das zugehörige policy reference file durch einen HTML `<link>` Tag anzugeben. Nachteil dabei ist, daß man die HTML Seite in der dieses Tag steht, erst einmal holen muß. Werden dann schon auf der Seite, in deren Quelltext das `<link>` Tag steht, Informationen gesammelt, kann dies noch nicht mit P3P angegeben werden. In Beispiel 3 ist die entsprechende HTML-Zeile zu sehen.

```
<link rel="P3Pv1" href="http://foo.bar/w3c/p3p.xml">
```

Beispiel 3: HTML `<link>` Tag zur Angabe des policy reference file

Damit bietet der Web-Server von der technischen Seite her schon P3P-Unterstützung. Das eigentliche Problem liegt in der Erstellung der notwendigen Dateien. Um hier den Unternehmen zu helfen, gibt es P3P Policy Generatoren, die mittels Multiple-Choice-Fragen die nötigen Dateien erzeugen. Bild 1 veranschaulicht diesen Prozess.

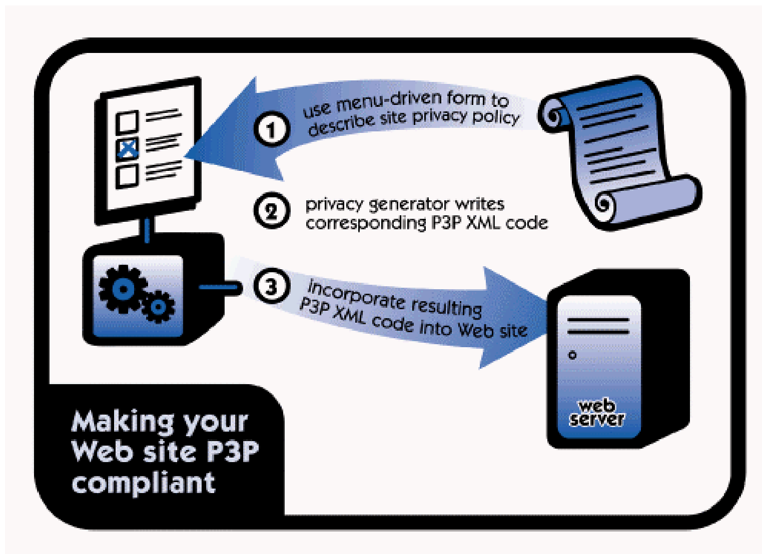

Bild 1: Generatoren helfen bei der Erzeugung der P3P Dateien

Im "policy reference file" sind Verweise auf die eigentlichen P3P policies zu finden, welche URLs durch sie abgedeckt werden, welche nicht und die Zeitspanne, für die diese Angaben gelten.

2.1.2. Clientseite

P3P muß in den Browser implementiert sein oder als Plugin geladen werden. Die Clients holen und lesen automatisch P3P-Policies und vergleichen sie mit den lokalen Benutzer-Eintellungen oder national gültigen Gesetzen im Land des Benutzers. Als nächstes holen sie die eigentliche Web-Seite und entscheiden dann ob die Seite normal dargestellt wird oder nicht.

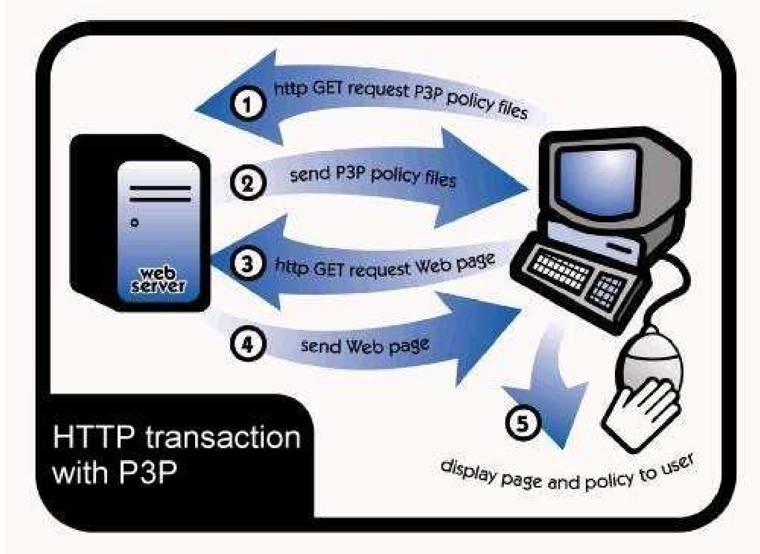

Bild 2: HTTP Transaktion mit P3P

Der Browser informiert den Benutzer über die Policies der gerade geholten Seite, falls diese seinen eingestellten privacy preferences widersprechen bzw. nicht mit ihnen zu vereinen sind. Andernfalls könnte man ein kleines Icon einblenden um zu signalisieren, daß P3P Dateien gefunden wurden und die Einstellungen des Anbieters mit den lokalen übereinstimmen. Bild 3 zeigt hierfür ein Beispiel.

Bild 3: Browser-Icon als Signal für aktiviertes P3P

Dadurch weiß man, daß die Seite zwar P3P unterstützt, aber im Moment keine Konflikte zwischen den gerade geholten Regeln und den lokalen Benutzer-Einstellungen bestehen.

2.2. Identifikation der Web-Site

In P3P existiert das <ENTITY> XML-Sprachelement, das Postadresse, E-Mail, Telefon, etc. angibt, um sich als Firma oder Unternehmen gegenüber dem Kunden zu identifizieren. Es steht in einer P3P-Policy genau einmal und kann wie in Bsp. 4 aussehen.

```
<ENTITY>
  <DATA-GROUP>
    <DATA ref="#business.name">Beispielkatalog</DATA>
    <DATA ref="#business.contact-info.postal.street">Hauptstrasse 23</DATA>
    <DATA ref="#business.contact-info.postal.city">Kaiserslautern</DATA>
    <DATA ref="#business.contact-info.postal.stateprov">RP</DATA>
    <DATA ref="#business.contact-info.postal.postalcode">67663</DATA>
    <DATA ref="#business.contact-info.postal.country">Germany</DATA>
    <DATA ref="#business.contact-info.online.email">info@foo.de</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.intcode">49</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.loccode">631</DATA>
    <DATA ref="#business.contact-info.telecom.telephone.number">123456</DATA>
  </DATA-GROUP>
</ENTITY>
```

Beispiel 4: <ENTITY> Element zur Identifikation

In Beispiel 4 geht es um ein Unternehmen namens "Beispielkatalog", seßhaft in Kaiserslautern, erreichbar per E-Mail und Telefonnummer wie oben angegeben. Die möglichen Datenelemente können im Kapitel 5.3.x der P3P Spezifikation vom W3C [7] nachgelesen werden.

2.3. Informationsklassifizierung

Um als Webseiten-Betreiber anzugeben, *welchen Typ* von Information man von den Benutzern sammelt, benutzt man in P3P das <STATEMENT> Element, von dem in jedem Policy-File mindestens eines vorhanden sein muß.
In Beispiel 5 wurde angegeben, daß Clickstream-Information und Browser-Programmname gesammelt wird (<DATA-GROUP>), dies nur zu Administrations- und Verbesserungszwecken der aktuellen Seite benutzt wird (<PURPOSE>), an keine Dritten weitergegeben wird (<RECIPIENT>) und die Daten nur für eine kurze, irgendwo anders in leicht verständlicher Form angebener Zeitspanne, gespeichert und danach gelöscht werden (<RETENTION>).

```
<STATEMENT>
  <CONSEQUENCE>
    We record some information in order to serve your request
    and to secure and improve our Web site.
  </CONSEQUENCE>
  <PURPOSE><admin/><develop/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#dynamic.clickstream.server"/>
    <DATA ref="#dynamic.http.useragent"/>
  </DATA-GROUP>
</STATEMENT>
```

Beispiel 5: `<STATEMENT>` Element (1)

Bei `<DATA ref="#..."/>` kann man die selben Datentypen wie beim `<ENTITY>` Tag angeben. `<CONSEQUENCE>` beschreibt kurz den Grund des Sammelns der Daten. Ein anderes Beispiel für die Benutzung des `<STATEMENT>` Elements –denkbar als Policy bei einem Online-Shop– wäre, anzugeben, daß man Namen, Postadresse, Firmenpostadresse, Telefon, Firmentelefon, E-Mail und diverse Informationen über Produkt, das der Kunde kauft, sammelt (`<DATA-GROUP>`). Dabei wird die Information nur gebraucht, um die aktuelle Transaktion zu vervollständigen (`<PURPOSE>`) und geht nur an die (weiter oben im `<ENTITY>` tag angegebene) Firma der Web-Seite selbst (`<RECIPIENT>`). Wieder werden die Daten nur für eine kurze, irgendwo anders näher erläuterte Zeitspanne, gespeichert und danach gelöscht (`<RETENTION>`). Der entsprechende XML Code ist in Beispiel 6 zu sehen.

```
<STATEMENT>
  <CONSEQUENCE>
    We use this information when you make a purchase.
  </CONSEQUENCE>
  <PURPOSE><current/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#user.name"/>
    <DATA ref="#user.home-info.postal"/>
    <DATA ref="#user.home-info.telecom.telephone"/>
    <DATA ref="#user.business-info.postal"/>
    <DATA ref="#user.business-info.telecom.telephone"/>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.miscdata">
      <CATEGORIES><purchase/></CATEGORIES>
    </DATA>
  </DATA-GROUP>
</STATEMENT>
```

Beispiel 6: `<STATEMENT>` Element (2)

2.4. Zweck des Sammelns der Kundeninformation

Zur Angabe des Grundes des Sammeln der Kundeninformationen läßt P3P beliebige Kombinationen aus den Werten aus Tabelle 1 zu. Diese Werte werden im <PURPOSE> Element benutzt; Mehrfachnennung eines Wertes ist erlaubt, jedoch ohne Bedeutung. Die <PURPOSE> Angabe steht innerhalb eines <STATEMENT> Elements, wie oben in Beispiel 6 gezeigt.

Wert	*Bedeutung / Übersetzung*
`<current/>`	Fertigstellung und Unterstützung der aktuellen Aktivität
`<admin/>`	Web-Seiten- und Systemadministration
`<develop/>`	Forschung und Entwicklung
`<customization/>`	bestätigende Anpassung
`<tailoring/>`	One-time Tailoring (nicht näher erläutert)
`<pseudo-analysis/>`	Pseudoanalyse
`<pseudo-decision/>`	Pseudoentscheidung
`<individual-analysis/>`	Analyse eines Individuums
`<individual-decision/>`	Entscheidung aufgrund eines Individuums
`<contact/>`	Kontaktaufnahme für Marketing-Zwecke
`<historical/>`	historische Erhaltung
`<telemarketing/>`	Telefonhandel
`<other-purpose>` Zweck `</other-purpose>`	Anderes, anzugeben durch "Zweck"

Tabelle 1: mögliche Werte des <PURPOSE> Elements

Wie man sieht, zielt P3P darauf ab, ziemlich genau anzugeben, wann Informationen gesammelt werden, um wirklich einen Kunden persönlich identifizieren und analysieren zu können (<individual-analysis/>), damit der Kunde ganz klar und eindeutig vom Browser gewarnt werden könnte, wenn er dies im Browser eingestellt hat. Andere Werte wie <tailoring/> und <historical/> lassen viel Interpretationsspielraum zu; sie sind in der P3P Spezifikation nicht näher erläutert.

2.5. Weitergabe von Informationen

Um anzugeben, an wen die gesammelten persönlichen Informationen weitergegeben werden, ist in P3P das <RECIPIENT> Tag vorgesehen. Damit werden die Empfänger in die in Tabelle 2 aufgelisteten Klassen unterteilt.

Wert	*Bedeutung / Übersetzung*
`<ours/>`	nur wir und unsere Mitarbeiter
`<same/>`	legale Einheiten die nach unseren Prinzipien handeln
`<other-recipient/>`	legale Einheiten die nicht nach unseren Prinzipien handeln
`<delivery/>`	Lieferservices, die nicht nach unseren Prinzipien handeln
`<public/>`	öffentliches Forum
`<unrelated/>`	nicht verwandte Dritte

Tabelle 2: mögliche Werte des <RECIPIENT> Elements

Hat also ein Kunde im Browser eingestellt, daß er gewarnt werden will, falls seine Telefonnummer an Dritte weitergegeben wird, sollte der Browser z.B. ein Popup darstellen, falls im zur Telefonnummer gehörenden <RECIPIENT> Feld "<delivery/>" oder "<unrelated/>" steht. Es sind wieder beliebige Kombinationen der oben stehenden sechs Werte möglich.

2.6. Verstöße gegen P3P-Abmachungen

Damit man angeben kann, welche Maßnahmen der Betreiber unternimmt oder anbietet, wenn er nun doch gegen das verstößt, was er in seinen P3P-Policies verspricht, also z.B. nun doch die E-Mail Adresse an Dritte weitergibt obwohl er das Gegenteil in seinen P3P-Policies versprochen hat, gibt es für ein Policy file das Tag <DISPUTES-GROUP>, in dem wiederum mindestens ein <DISPUTES> Element und optional <REMEDIES> Elemente vorkommen können.
Hierzu nehmen wir folgende Situation an: Eine Firma möchte für Konfliktfälle oder Bruch eines Versprechens das in P3P gegeben wurde Folgendes zum Ausdruck bringen: *"Falls wir nicht auf Ihre Beschwerde geantwortet haben oder Ihre Anfrage nicht zufriedenstellend behandelt wurde, können Sie PrivacySealExample unter http://www.privacyseal.example.org kontaktieren. Wir werden alle Fehler oder falsche Handlungen in Zusammenhang mit der P3P Policy beheben."* Die entsprechende P3P Notation ist in Beispiel 7 zu sehen.

```
<DISPUTES-GROUP>
  <DISPUTES resolution-type="independent"
    service="http://www.PrivacySeal.example.org"
    short-description="PrivacySeal.example.org">
    <IMG src="http://www.PrivacySeal.example.org/Logo.gif"
         alt="logo"/>
    <REMEDIES><correct/></REMEDIES>
  </DISPUTES>
</DISPUTES-GROUP>
```

Beispiel 7: Lösen von Konflikten, Beschwerden und Zweifelsfällen

Optional könnte innerhalb des <REMEDIES> Elements als Reaktion auf eine Zuwiderhandlung auch <money/> stehen, etwa so: <REMEDIES> <money/> </REMEDIES>, um auszudrücken, daß jemand mit einem angemessenen Betrag Geld entschädigt wird um den durch Weitergabe von persönlicher Information entstandenen Schaden wettzumachen. Was "angemessen" ist steht in der menschlich-lesbaren Form der Politik dieses Unternehmens.
Alternativ könnte man statt <money/> auch noch <law/> angeben, was bedeutet daß das lokale Gesetz des Landes zur Entscheidungsfindung in diesem Fall eingeschaltet wird.

2.7. Leicht verständliche Kurzbeschreibung für die Sammlung von Daten

Wie in einigen vorhergehenden Beispielen schon zu sehen ist, ist es möglich und empfehlenswert bei jedem <STATEMENT> eine für den Menschen bestimmte Beschreibung mit anzugeben, die dann in eventuell anzuzeigenden Popups verwendet werden kann. Beispiel 8 ist eine Möglichkeit die ein Betreiber eines Online-Shops gewählt haben könnte.

```
<CONSEQUENCE>
  We use this information when you make a purchase.
</CONSEQUENCE>
```

Beispiel 8: <CONSEQUENCE> Element

2.8. Cookies

Alle angesprochenen Regeln können nicht nur für durch Formulardaten oder schlichtes Surfen entstandene Daten, sondern auch für cookies verwendet werden. Dies wird im policy reference file angegeben, wobei man hier nun z.B. statt dem bekannten Konstrukt für HTML Seiten, wie es in Beispiel 9 zu sehen ist eine ähnliche Zeile für cookies angibt, so wie in Beispiel 10.

```
<META xmlns="http://www.w3.org/2000/12/P3Pv1">
  <POLICY-REFERENCES>
    <POLICY-REF about="/p3p/Policy1.xml">
      <INCLUDE>/*</INCLUDE>
    </POLICY-REF>
  </POLICY-REFERENCES>
</META>
```

Beispiel 9: policy reference file für HTML Seiten

```
<META xmlns="http://www.w3.org/2000/12/P3Pv1">
  <POLICY-REFERENCES>
    <POLICY-REF about="/P3P/CookiePolicy1.xml">
      <COOKIE-INCLUDE>* * *</COOKIE-INCLUDE>
    </POLICY-REF>
  </POLICY-REFERENCES>
</META>
```

Beispiel 10: policy reference file für cookies

In Beispiel 10 wird für alle cookies die Policy `/P3P/CookiePolicy1.xml` angewendet. Die drei Parameter (hier mit `*` angegeben) innerhalb von `<COOKIE-INCLUDE>` sind *Name*, *Domäne* und *Pfad* des cookies.
Äquivalent zum `<EXCLUDE>` Element gibt es für cookies ein entsprechendes `<COOKIE-EXCLUDE>` Element um cookies genauer in Klassen unterteilen zu können, wie im Beispiel 1 bei HTML Seiten deutlich gemacht. So kann man exakt die Teilmengen umschreiben, die man für eine Policy haben will.

3. Bewertung

3.1. Was P3P nicht kann:

P3P kann keine Minimalanforderungen an die Sicherheit stellen bzw. erfüllen und garantieren, daß sich Betreiber einer Web-Site wirklich an die Versprechen auf seinem "Aushängeschild" zur Privatsphäre hält. Zum Beispiel könnten die Anbieter trotzdem E-Mail-Adresslisten erstellen und diese an Werbungsunternehmen weiterverkaufen auch wenn sie dies nicht so in Ihren P3P policies offenlegen. P3P basiert also letztendlich doch wieder nur auf das Vertrauen des Web-Nutzers gegenüber dem Dienstleister. Wenn eine Web-Seite mehrere Jahre zuverlässig keine Informationen über die dort surfenden Nutzer preisgibt (doch wie überprüft man, ob wirklich nichts an Dritte durchsickert ?) wird sich wohl eine gewisse Vertrautheit einstellen.
Es wäre Aufgabe einer entsprechend komplementären Gesetzgebung und Strafverfolgung, die Anbieter an Ihre Versprechen zu binden und Mißstände bei Datenschutzpraktiken aufzudecken.
P3P kann aber dabei helfen, Benutzer für das Thema Datenschutz zu sensibilisieren und bestehende Mißstände bei Datenschutzpraktiken einzelner Anbieter aufzudecken. Mit der Existenz solcher Protokolle werden Nutzer aufmerksam auf das bestehende Problem gemacht. Damit ist P3P nur ein möglicher integraler Baustein für eine umfassendere Datenschutzlösung im WWW neben den oben erwähnten Anonymiser-Werkzeugen.

3.2. Ausblick in die Zukunft

Im Prinzip ist P3P keine schlechte Idee, was aber zur Zeit noch fehlt, ist die konsequente Implementierung von P3P in die bekannten Browser Netscape und Internet Explorer (IE). Microsoft behauptet zwar, daß im aktuellen IE 6 Beta P3P unterstützt werden soll, aber alles was der IE macht, ist nach meinen Untersuchungen einfach nur, cookies in "akzeptabel" und "inakzeptabel" zu unterteilen. Von Pop-Up Nachrichten auf den Test-Sites die ich untersucht habe (vom W3C und selbst erstellte), ist nichts zu sehen.
Außerdem fehlt die nötige Gesetzgebung und Strafverfolgung komplett. Bis P3P mit in die Gesetze aufgenommen durchsetzt – dazu noch in allen Ländern der Erde – wird wohl noch viel Zeit vergehen, wenn es überhaupt so weit kommt. Natürlich wäre es schon ein großer Fortschritt, wenn nur in Deutschland P3P verbreitet wäre, allerdings ist Deutschland ja für seine langen bürokratischen

Wege berühmt berüchtigt. Ein Qualitätsmerkmal, das deutsche Geschäfte dann gegenüber französischen oder amerikanischen Online-Shops hätten, wäre P3P aber allemal und würde eventuell Kunden zu Anbietern mit P3P Unterstützung locken.
Andererseits können zwielichte Unternehmen mittels P3P alles mögliche über die Achtung der Privatsphäre behaupten, dies letztendlich doch nicht einhalten und Informationen hinter dem Rücken des Nutzers an Werbeunternehmen weitergeben. Große, namhafte Firmen wie IBM oder AT&T werden dies sehr wahrscheinlich nicht tun, um nicht an positivem Eindruck und Vertrauen der Kunden zu verlieren. Jedoch kann kein Nutzer in akzeptabler Zeit und mit vertretbarem Aufwand nachprüfen, was hinter deren Türen alles geschieht.
Es gibt schon eine Reihe Web-Seiten, die laut W3C P3P implementiert haben, zu lesen unter `http://www.w3.org/P3P/compliant_sites`. Dabei sind bekannte wie IBM [8], AOL [9] oder Microsoft [10], mittelgroße Institutionen (Schulen) und auch einfache private Homepages von einzelnen, eher unbekannten Personen.

4. Zusammenfassung

P3P ist ein auf XML basierendes, auf HTTP aufsetzendes Protokoll zur Modellierung von Regeln zwischen Web-Seiten-Betreibern und deren Kunden. Diese Regeln geben an, wie die Informationen, die der Kunde über seine eigene Person offenbart, behandelt werden. Damit die Regeln maschinenlesbar sind, werden sie mittels Generatoren oder von Hand in XML Dateien geschrieben, auf dem Server abgelegt und dann immer wieder von den Clients, die P3P unterstützen abgeholt. Im zweiten Teil wurde eine Übersicht über die wichtigsten Sprachelemente gegeben und deren Bedeutung anhand vieler Beispiele erklärt. Zum Schluß wurde das Ganze bewertet.

5. Literatur

[1] Freedom – Internet Privacy Software. © 1999 by Zero-Knowledge – http://www.zks.org/

[2] AltaVista – The Search Company. Internet-Suchmaschine – http://www.altavista.com/

[3] DoubleClick – Die Experten für Internetwerbung – http://www2.doubleclick.net/de/

[4] Heise Verlag AG: Newsticker – http://www.heise.de/newsticker/data/daa-18.06.01-000/

[5] IBM P3P Policy Editor – http://www.alphaworks.ibm.com/tech/p3peditor

[6] PrivacyBot – http://www.privacybot.com/

[7] The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Candidate Recommendation 15 December 2000 – http://www.w3.org/TR/P3P/

[8] IBM – Industrial Business Machines – http://www.ibm.com/

[9] AOL – America Online – http://www.aol.com/

[10] Microsoft Net – http://www.msn.com/