P3P - Ein neuer Standard für Datenschutz im Internet

Marc Langheinrich
Institut für Informationssysteme
ETH Zürich

<langhein@inf.ethz.ch>

Das internationale World Wide Web Consortium (W3C) hat im April 2000 einen neuen Web-Standard für bessere Transparenz im Online-Datenschutz vorgestellt: das "Platform for Privacy Preferences Project" (P3P). P3P beinhaltet ein (maschinenlesbares) Vokabular zur Beschreibung von Datenschutzpraktiken einer Website, sowie ein Protokoll zum automatischen Austausch dieser Beschreibung mit dem Web-Browser eines Besuchers. Statt seitenweise Kleingedrucktes zu lesen, können Benutzer mittels P3P sämtliche Informationen über die Verwendung ihrer Daten in übersichtlichen, standardisierten Dialogen ihres Browsers überprüfen und gemäss ihren Präferenzen automatisch akzeptable Web-Seiten von inakzeptablen unterscheiden.

Einleitung

Eine alte Internet-Weisheit besagt: "On the Internet, nobody knows you're a dog". Dass von dieser Möglichkeit auch im Zeitalter des World Wide Web noch immer viele Benutzer Gebrauch machen, beweist die kontinuierliche Nachfrage nach Anonymisier-Werkzeugen, wie beispielsweise Anonymizer.com [1] oder der "Freedom"-Software von Zero-Knowledge [2]. Doch nicht immer macht anonymes Surfen Sinn - in vielen Situationen ist die Preisgabe persönlicher Daten nützlich oder sogar notwendig: Seien es personalisierte Online-Terminkalender, -Horoskope oder -Adressbücher – erst durch die Eingabe persönlicher Daten lassen sich diese Angebote sinnvoll nutzen. Und aller Online-Einkauf ist nutzlos, wenn dem Anbieter nicht auch die Lieferadresse angegeben wird.

In solchen Situationen, in denen sich selbst der vorsichtigste Benutzer entschliessen dürfte, doch einmal ein Web-Formular auszuzfüllen, ist es wichtig, dass er sich die Konsequenzen dieser Angaben klar machen kann: wer erhält meine Daten (nur der Anbieter selber, oder werden sie an Dritte weitergegeben?), zu welchem Zweck werden sie erhoben (geht es nur um die Erfüllung meiner Bestellung, oder werden sie auch zu Marketingzwecken verwendet?),

und welche Möglichkeiten des Zugriffs habe ich später (d.h. kann ich meine eingegebenen Daten ändern oder sogar löschen)?

Hier setzt P3P [3] an, welches zum Ziel hat, das Veröffentlichen von Datenschutzpraktiken und deren anschliessende Beurteilung durch den Benutzer zu vereinfachen. P3P kann keine Garantien geben, dass Anbieter sich auch wirklich an die von ihnen veröffentlichten Praktiken halten - dies ist Aufgabe einer entsprechend komplementären Gesetzgebung und Strafverfolgung. P3P kann aber dabei helfen, Benutzer für das Thema Datenschutz zu sensitivieren und bestehende Missstände bei Datenschutzpraktiken einzelner Anbieter aufzudecken. Damit ist es, neben den oben erwähnten Anonymisier-Werkzeugen, ein integraler Baustein für eine umfassende Datenschutzlösung im Internet.

Das P3P-Prinzip

Die Idee von P3P ist recht einfach: ein Anbieter im Web übersetzt seine Datenschutzpraktiken - d.h. eine Auflistung der Daten, die er vom Besucher erhebt, sowie deren Empfänger, Verwendungszweck, etc. - in ein standardisiertes XML-Format [4] und veröffentlicht dieses auf seiner Website. Benutzer, die diese Website mittels eines P3P-fähigen Browsers besuchen, können sich die Praktiken dann komfortabel in übersichtlichen Dialogen ansehen und selbst entscheiden, ob sie unter diesen Bedingungen gewillt sind, ihre persönlichen Daten auszugeben. Haben sie einmal ihre diesbezüglichen Präferenzen in ihrem Browser eingestellt, kann dieser ihnen diese Entscheidung weiter vereinfachen, indem er auomatisch Websites in "aktzeptabel" und "inakzeptabel" einteilt. Fallen die Praktiken der Website ausserhalb der Präferenzen des Benutzers, können zusätzliche Informationen und Warnungen eingeblendet werden, um die unerwünschte Preisgabe der persönlichen Daten zu verhindern.

Komponenten von P3P

Damit all dies reibungslos funktioniert, definiert die P3P-Spezifikation auf über 100 Seiten eine Reihe von Komponenten, die aufeinander aufbauend weit mehr als nur ein weiteres Internet-Protokoll darstellen:

- Daten-Schemata: Die P3P-Spezifikation definiert eine umfangreiche Menge von Datenarten, welche Web-Anbieter von den Besuchern ihrer Web Seiten erheben können, z.B. Nachname, Vorname, aber auch IP-Adresse, Cookies, etc.
- Praktiken-Vokabular: Mittels eines weitreichenden Vokabulars für die Offenlegung von Datenschutzpraktiken können Anbieter exakt aufschlüsseln, welche der obigen Daten sie wann, zu welchem Zweck und für wen erheben. Beispiele sind die Deklaration des Empfängers der Daten, deren Verwendungszweck und spätere Zugriffsmöglichkeiten.
- XML-Syntax: Damit die Datenschutzpraktiken maschinell ausgelesen und verarbeitet werden können, definiert P3P einen XML-Syntax, in der das P3P-Vokabular auf die Daten-Schemata angewendet werden können.

- Protokoll: Die so in einer XML-Syntax niedergeschriebenen Datenschutzpraktiken werden über ein effizientes Protokoll mit Web-Inhalten verknüpft (d.h. HTML-Seiten, aber auch Grafiken oder Musik-Dateien) und über HTTP transportiert.
- Präferenz-Sprache ("A Privacy Preferences Exchange Language" - APPEL [5]): Eine separate Regelsprache erlaubt Benutzern die flexible Formulierung ihrer Präferenzen, anhand derer Datenschutzpraktiken in "akzeptabel", "bedingt akzetabel" oder "nicht akzetabel" eingeteilt werden können. Durch die Standardisierung können solche Präferenzen über verschiedene Produkte und Anbieter hinweg ausgetauscht werden.

Über einen Zeitraum von mehr als drei Jahren konzipierte eine internationale Arbeitsgruppe von zeitweise bis zu 50 Mitgliedern unter der Führung von Tim Berner-Lee's W3C [6] mit P3P ein "Social Protocol", bei dem sowohl technische, rechtliche, wie auch soziale Aspekte eine Rolle spielen. Mit Teilnehmern von international tätigen Organisationen, Universitäten, Verbraucherschutzgruppen und Datenschutzbeauftragten aus Europa, Amerika und Asien wurde versucht, einen breiten Konsens über die verschiedensten Interessensgruppen hinweg zu finden. Dies erklärt auch die relativ lange Zeitspanne, welche zwischen Gründung der Arbeitsgruppe und der Veröffentlichung der ersten Spezifikation verstrich.

P3P in der Praxis

Ein Hauptschwerpunkt bei der Entwicklung von P3P war das Ziel, P3P sowohl für Anbieter als auch Benutzer attraktiv zu machen. In Zusammenarbeit mit Datenschutzbeauftragten und Verbraucherorganisationen weltweit wurde ein umfassendes Vokabular erstellt, welches eine maximale Transparenz gängiger Datenschutz-Praktiken anstrebt, um diese sowohl wahrheitsgetreu als auch verständlich dem Benutzer zugänglich zu machen.

Um eine rasche Verbreitung in der Praxis zu ermöglichen und die für Internet-Technologien so lebenswichtige Akzeptanz bei Software-Herstellern, Netzbetreibern und Anbietern zu gewährleisten, wurde das Kommunikationsprotokoll in P3P bewusst einfach gehalten. Dies minimiert sowohl die Belastungen für die genutzten Kommunikationskanäle (damit Download-Zeiten nicht durch den Einsatz von P3P unnötig verzögert werden), als auch den nötigen wirtschaftlichen Einsatz: P3P in seiner ersten Version (P3P1.0) kann ohne Software-Änderungen in fast alle gängigen kommerziellen und kostenfreien Web Server integriert werden - ein wichtiger Aspekt für eine schnelle anfängliche Verbreitung von P3P-unterstützenden Websites.

Für den Benutzer selbst soll die Verwendung von P3P ebenfalls so einfach wie möglich gemacht werden. Ausser einem mehr oder weniger unauffälligen Indikator, welcher die aktivierte P3P-Unterstützung anzeigt, sollte sich das Besuchen von Web-Angeboten mit P3P kaum vom heutigen, P3P-losen Surfen unterscheiden. Lediglich im Falle einer Website mit ungenügenden oder fragwürdigen Datenschutzpraktiken (bezogen auf die individuellen Präferenzen des Benutzers) können auf Wunsch des Benutzers zusätzliche Informationen, wie z.B. Warnsymbole, Statusanzeigen oder Dialogboxen, eingeblendet werden.

Ob akzeptabel oder nicht akzeptabel - mit P3P hat der Benutzer jederzeit die Möglichkeit, die momentan gültigen Praktiken einer Website in einem übersichtlichen, standardisierten Format zu inspizieren. So könnte beispielsweise beim Ausfüllen von Web-Formularen individuell der Empfänger und der Verwendungszweck jedes einzelnen Feldes mittels eines Maus-Clicks

abgefragt werden. Ebenso möglich ist eine Journal-Funktion, welche für den Benutzer über alle ausgegebenen Daten detailliert Buch führt: wann wurde welche Information an wen zu welchen Konditionen ausgegeben, und wie kann ich meine Daten beim Anbieter später ändern oder löschen?

Ausblick

P3P scheint auf den ersten Blick ein stark auf US-amerikanische Verhältnisse zugeschnittenes Werkzeug zu sein. Insbesondere die Verabschiedung der EU Datenschutz-Direktive (Direktive 95/46/EC, [7]) suggeriert, dass in Europa kein direkter Bedarf für eine solche Datenschutz-Plattform besteht. Dennoch ist P3P gerade *wegen* dieser Direktive äusserst interessant für Europa: Eine konsequente Verwendung von P3P-unterstützenden Produkten ermöglicht dem Verbraucher erst die in der Direktive geforderte Transparenz bei der Datenerhebung - ein notwendiges Werkzeug für die Umsetzung der Gesetze also. Ebenso erlaubt es sowohl europäischen wie auch aussereuropäischen Benutzern einen direkten Vergleich zwischen verschiedenen gängigen Datenschutzpraktiken in den verschiedensten Bereichen der Welt und macht so Datenschutz zu einem Wettbewerbs-Vorteil.

Wichtig ist, dass man bei der Beurteilung von P3P die Ziele dieses Projektes nicht aus den Augen verliert: P3P ist keine "Komplettlösung", sondern nur in Zusammenhang mit anderen Komponenten ein wirkungsvoller Schritt zum umfassenden Datenschutz im Internet. Gütesiegel-Programme, wie beispielsweise TRUSTe [8] oder BBBOnLine [9], können helfen, in Ländern ohne adäquate Gesetzgebung Firmen zur Aufrechterhaltung ihrer Datenschutzpraktiken zu zwingen und dadurch Benutzern ein Mindestmass an Absicherung bieten. Anonymisier-Werkzeuge, wie Anonymizer.com oder Zero-Knowledge's Freedom, erlauben das Surfen in Anonymität, immer dann, wenn persönliche Daten (dazu können sogar IP-Adressen zählen) nicht notwendig sind. Verschlüsselungstechnologien ermöglichen sicheren Transfer und Speicherung der Daten und erlauben in begrenztem Masse (durch digitale Signaturen) die verlässliche Nichtabstreitbarkeit. Eine umfassende Gesetzgebung bietet schlussendlich eine wirkungsvolle Grundlage für akzeptable Datenschutzpraktiken.

Obwohl viele Teile des Puzzles noch in weiter Ferne zu liegen scheinen, ist mit P3P sicherlich ein erster Schritt in die richtige Richtung getan. Mehrere Firmen haben bereits ihre Datenschutzpraktiken im P3P-Format veröffentlicht (z.B. AOL, AT&T, IBM, HP und Microsoft) oder planen bzw. arbeiten bereits an P3P-fähigen Werkzeugen (z.B. Microsoft, IDecide, oder YOUpowered). Sobald diese Programme der breiten Öffentlichkeit zur Verfügung stehen, wird es sich zeigen, ob Benutzer von ihren neuen Möglichkeiten zum individuellen Datenschutz auch in dem Masse profitieren können, wie Verbraucherschützer es sich erhoffen.

Weitere Informationen

Die Seiten des W3C bieten unter `www.w3.org/P3P/` eine umfassende Übersicht über P3P, mit Querverweisen auf die Spezifikationen, Links auf P3P-unterstützende Websites und Produkte, eine Liste der am häufigsten gestellten Fragen und ihrer Antworten ("FAQ"), sowie Hintergrundinformationen zum Thema Datenschutz im Internet.

Über den Autor

Marc Langheinrich ist seit Oktober 1997 Mitglied der P3P-Arbeitsgruppe und Mitautor der P3P- und APPEL-Spezifikation. Seit Oktober 1999 ist er wissenschaftlicher Mitarbeiter am Institut für Informationssysteme der ETH Zürich. Seine Homepage befindet sich unter `www.inf.ethz.ch/~langhein/`

Literatur

[1] *Anonymizer.com - Online Privacy Services.* Siehe `www.anonymizer.com`

[2] *Freedom - Internet Privacy Software.* (C) 1999 by Zero-Knowledge. Siehe auch `www.zks.org`

[3] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Joseph Reagle: *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification,* W3C Working Draft. HTML-Version siehe `www.w3.org/TR/P3P`

[4] Tim Bray, Jean Paoli, C.M. Sperberg-McQueen, Eve Maler: *Extensible Markup Language (XML) 1.0 (Second Edition),* W3C Recommendation. HTML-Version siehe `www.w3.org/TR/2000/REC-xml-20001006`. Weitere Informationen über XML finden sich unter `www.w3.org/XML/`

[5] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori: *A Privacy Preferences Exchange Language 1.0 (APPEL1.0) Specification,* W3C Working Draft. HTML-Version siehe`www.w3.org/TR/WD-P3P-preferences`

[6] *The World Wide Web Consortium (W3C).* Die Homepage findet sich unter `www.w3.org`

[7] *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 - 0050. Zu finden unter der Homepage der Arbeitsgruppe für Medien, Informationsgesellschaft und Datenschutz: `europa.eu.int/comm/internal_market/de/media/dataprot/index.htm`

[8] *TRUSTe: Building a Web You Can Believe In.* Homepage unter `www.truste.org`

[9] *BBBOnLine, Inc. – Promoting Trust and Confidence on the Internet.* Homepage unter `www.bbbonline.com`