Privacy UX – Was ist datenschutzbezogene User Experience?

Michael Hatscher
Google Switzerland
Brandschenkestrasse 110
8002 Zürich
mitchhatscher@google.com

Sebastian Schnorf
Google Switzerland
Brandschenkestrasse 110
8002 Zürich
sebschnorf@google.com

Martin Ortlieb
Google Switzerland
Brandschenkestrasse 110
8002 Zürich
mortlieb@google.com

Kalle Kormann-Philipson
Google Germany
Dienerstraße 12
80331 München
kalle@google.com

Abstract
Angeregte Diskussionen in Presse und Politik sowie aktuelle Gesetzgebungsprozesse, wie die im Mai in Kraft getretene E-Privacy- Direktive oder die im Reviewprozess befindliche Datenschutz-Rahmenrichtlinie, weisen auf die hohe und weiter steigende Bedeutung von Datenschutz auch im Internet hin. Damit wird Privacy UX ein Thema, dem sich Usability Professionals in allen Unternehmen stellen müssen, die Nutzerdaten verarbeiten. Am Beispiel von Googles Privacy UX-Team zeigen wir auf, was a) unsere Arbeit von derjenigen anderer Usability Professionals unterscheidet, b) in welchem Kontext wir uns bewegen und c) wie wir die Qualität unserer Arbeit zu messen versuchen. Wir berichten über ein ehrgeiziges User Research-Projekt und wie sich die so gewonnenen Erkenntnisse in den Produkten niederschlagen konnten. Abschließend führen wir Faktoren für erfolgreiche Privacy UX-Arbeit auf und zeigen einige Lessons Learned auf.

Keywords:
/// Datenschutz
/// Privacy Policy
/// Privacy UX
/// UX-Aufgabenfelder
/// Privacy UX-Messkriterien

1. Einleitung: Warum datenschutzbezogene UX?

User Experience für Datenschutzprodukte und -services (Privacy UX) ist ein neues Tätigkeitsfeld für User Experience Professionals, das rapide an Bedeutung gewinnt. Neben den Bedürfnissen der Nutzer kommen starke Impulse auch von zwei neuen rechtlichen Rahmenwerken, die für viel Diskussionsstoff sorgen: die gerade neu in Kraft getretene EU E-Privacy-Direktive und die sich noch im Reviewprozess befindende EU-Datenschutz-Rahmenrichtlinie, die in eine Verordnung übergehen soll. Privacy UX unterscheidet sich von „herkömmlicher" produktbezogener UX-Arbeit in mehrerer Hinsicht:

- Privacy UX erstreckt sich meist über einzelne Produkte hinweg bzw. liegt quer zu ggf. bestehenden Produktgruppen oder -silos
- Privacy UX richtet sich nach innen (interne Datenverarbeitungsprozesse) und nach außen (Datenschutzprodukte für Nutzer)
- Privacy UX bearbeitet ein Feld, in dem Metriken für Erfolg fast vollständig fehlen. So ist nicht leicht zu erheben, wie und wann Privacy UX gute Arbeit geleistet hat.

Privacy UX findet in einem Umfeld mit unterschiedlichen Herausforderungen statt. Neue Produkt-Features, gerade bei „sozialen" Produkten, laden Nutzer oft dazu ein, möglichst viel über sich preiszugeben. Um neue Produkte zu realisieren, wäre es wünschenswert, wenn Daten möglichst frei bewegt werden können innerhalb eines Unternehmens oder des Ökosystems, in das ein Unternehmen eingebettet ist. Auch bestehen in verschiedenen Ländern unterschiedliche Rechtsauffassungen, Gesetze und Traditionen zum Thema Datenschutz und Privatsphäre, die bestimmen, wie mit privaten Daten umgegangen werden soll und darf. Da Daten aber nicht an einen Ort oder an Staatsgrenzen gebunden und viele Unternehmen international tätig sind, benötigt man rechtliche Rahmenwerke, damit Unternehmen nicht versehentlich geltendes Recht verletzen. Die zwischen der EU und den USA geltenden „International Safe Harbor Privacy Principles" definieren, wie US-Unternehmen mit Daten von EU-Bürgern umgehen müssen, um mit den EU-Datenschutzgesetzen in Einklang zu sein. Darüber hinaus behandeln die Medien Datenschutzthemen gern und nicht immer nur sachlich. Letztlich weisen auch Nutzerreaktionen und -verhalten eine große Varianz auf, die von Unbekümmertheit über Ratlosigkeit bis hin zu irrationalen Handlungen, „abergläubischem Verhalten" und Panik reicht. Vielfach konnte auch festgestellt werden, dass beim Thema „Datenschutz" zwischen Nutzereinstellung und eigentlichem Nutzerverhalten eine große Inkongruenz vorherrscht (z. B. Joinson, Reips, Buchanan & Paine Schofield, 2010; generell dazu: Fishbein & Aijzen, 1975)

Im folgenden Beitrag werden wir Privacy UX näher beschreiben und dabei beispielhaft auf das Google Privacy UX-Team verweisen. Es geht darum, welche Aufgaben Privacy UX umfasst, in welchem Maße umfangreiche User Research uns hilft, das Feld besser zu begreifen, und wie wir

Erfolgskriterien unserer Arbeit definieren. Abschließend listen wir eine Reihe von Faktoren auf, die wir als hilfreich für erfolgreiche Privacy UX-Arbeit identifiziert haben.

2. Datenschutzbezogene UX-Arbeit

Für die Tätigkeit im Umfeld der datenschutzbezogenen UX-Arbeit kann vor allem die geplante EU Datenschutzverordnung neue Anforderungen bringen, denn zusätzlich zu den bereits seit langem existierenden Rechten, wie z. B. dem Recht der Menschen zu erfahren, welche Daten über sie gespeichert sind, sollen noch weitere Prinzipien eingeführt werden:

- „Right to be forgotten": Daten von Nutzern sollten über ein Ablaufdatum verfügen.
- „Data portability": Der Umzug von Daten zwischen Anwendungen sollte gewährleistet werden.
- „Privacy by default": Einstellungen sollten standardmäßig nicht öffentlich sein.
- „Breach notification": Über die (unbeabsichtigte) Veröffentlichung von Daten sollte informiert werden.
- „Explicit consent": Nutzer sollten zur Verwendung ihrer Daten ihre Einwilligung geben.

Neben rechtlichen und infrastrukturbezogenen Implikationen bleibt offen, welche Auswirkungen diese Prinzipien konkret auf die Nutzer und ihr Nutzungserleben haben werden. Zum Beispiel: Wann, wo und mit welchen Features sollen Nutzer ihr Einverständnis (Consent) zur Verwendung personenbezogener Daten geben?

Bei Google gibt es bereits seit einigen Jahren eine Abteilung, die sich ausschließlich mit dem Thema Privacy beschäftigt. Das Privacy UX-Team innerhalb dieser Abteilung besteht aus einer Gruppe von User Experience Designern und User Experience Researchern, die zurzeit in Zürich, Mountain View und München ansässig sind. Wir arbeiten sehr stark mit Googles Privacy Engineering-Teams an diesen und weiteren Orten zusammen, halten aber auch engen Kontakt zu weiteren Abteilungen wie dem Legal-Department, der Policy-Abteilung und PR. Wir beschäftigen uns typischerweise mit den folgenden Fragestellungen:

- Wie kann für die Nutzer Transparenz erzeugt werden?
- Wie kann den Nutzern Kontrolle über ihre Daten gegeben werden?
- Wie kann man den Nutzern sinnvolle Wahlmöglichkeiten einräumen?

Diese Fragestellungen behandeln wir jeweils in Bezug auf a) Nutzerdaten, die bereits vorliegen, b) auf die zukünftige Nutzung von Daten, die erhoben werden sollen und c) auf den Umgang mit den Daten. Beispiele für konkrete Arbeitsgebiete und aktuelle Produkte sind:

- Google Dashboard: Nutzern Übersicht und Kontrolle über ihre Daten geben
- Google Anzeigenvorgaben-Manager: Nutzern Wahlmöglichkeiten bei der Personalisierung von Anzeigen verschaffen
- Google+ Circles: Nutzern verbesserte Möglichkeiten zum Teilen von Inhalten anbieten

Eine spannende Herausforderung besteht darin, dass es zum Thema Privacy sehr wenig verlässliche User Research-Ergebnisse gibt. Der Datenschutz-Diskurs wird vielfach innerhalb der Datenschutz-Szene durch Aktivisten, Technologen und Politiker betrieben. Die Medien greifen das Thema gern auf, weil es „gut funktioniert", Aufmerksamkeit und damit Klicks bzw. Schlagzeilen bringt – aber was genau ist es, was die Menschen zum Thema Datenschutz denken und fühlen? Um das zu verstehen, legten wir 2010 ein ehrgeiziges Datenschutz-Forschungsprojekt auf: User Perceptions of Privacy (UPOP).

3. Die Datenschutzbedenken unserer Nutzer verstehen: „User Perceptions of Privacy" (UPOP)

3.1. Das Forschungsprojekt

Das Forschungsprojekt „User Perceptions of Privacy", kurz UPOP, verfolgte zwei Zielsetzungen:

- Erforschen, was Nutzer unter „Datenschutz" verstehen. Wir wollten das Thema herauslösen aus einerseits der erhitzten Debatte unter Ingenieuren (Zugriffskontrolle, Verschlüsselung) und andererseits dem Diskurs unter den Juristen (Recht auf Privatsphäre, Konzept von Datenschutz als Abwenden von Unheil)
- Eine nutzerzentrierte Perspektive von „Datenschutz" gewinnen

Das Forschungsprojekt war wie folgt aufgebaut:

- Phase 1: Zuordnung von Terminologie und Kontext von Konversationen über Privatheit (durch 3 x 3 Fokusgruppen in verschiedenen Ländern bzw. Orten: London, Denver, München)
- Phase 2: Zusammentragen und Sammeln realer Nutzererfahrungen und Nutzerberichte zu speziellen privatheitsbezogenen Themen (~100 Tagebuchstudien in Großbritannien, Deutschland, US-West- und US-Ostküste)
- Phase 3: Eingehende Untersuchung über Strategien, wie Benutzer versuchen, sensible Daten zu schützen (34 In-Home Interviews in Großbritannien, Deutschland, US-Westküste, US-Ostküste)

3.2. Erkenntnisse aus der Forschung zu UPOP

Eines der zentralen Ergebnisse aus diesem Forschungsprojekt besteht darin, dass bestätigt werden konnte, dass Nutzer unter „Datenschutz" (oder Englisch „Privacy") vor allem die Einsicht in und die Kontrolle über ihre sensiblen Daten

verstehen. Einige der Erkenntnisse aus der UPOP-Forschung stellten auch für uns Überraschungen dar. So lassen sich beispielsweise praktisch keine prinzipiellen Unterschiede in den Datenschutz-Bedenken der Nutzer zwischen den USA, Großbritannien und Deutschland feststellen.

Weitere interessante Erkenntnisse sind unter anderem:

- Nutzer haben in erster Linie Sorge davor, dass andere, meist ihnen bekannte Menschen Zugriff auf ihre Daten bekommen; weniger Sorgen machen sie sich über Zugriffe durch Hacker. Noch deutlich weniger fürchten sie einen unberechtigten Zugriff durch Unternehmen oder staatliche Institutionen
- Nutzer haben nicht per se ein Problem damit, dass Daten über sie online verfügbar sind. Allerdings sind sie unglücklich über den fehlenden Überblick über diese oft scheinbar periphären Daten. Nutzer möchten wissen können, wer in welchem Maße auf was für Daten über sie Zugriff hat
- Weiterhin befürchten Nutzer, aufgrund von öffentlich zugänglichen Daten unfair bewertet zu werden (z. B. indem jemand von ihrem Musikgeschmack Rückschlüsse auf ihren Charakter zieht)
- Nicht nur im Rahmen von UPOP, sondern auch bei anderen User Research-Aktivitäten hören wir immer wieder, dass Nutzer sich von Google (und anderen großen Unternehmen der Branche) Hinweise, Hilfe und Strategien zum Umgang mit und zum Schutz privater Daten wünschen

Viele dieser Erkenntnisse haben auch direkt Einfluss auf Design- und Produktentscheidungen gefunden. Beispielsweise hatten sich Nutzer vor allem besorgt gezeigt über unberechtigten Zugriff auf ihre Daten durch andere, ihnen bekannte Menschen. Für Google Dashboard zogen wir daher einen zweiten Authentifizierungsschritt ein, um sicherzugehen, dass die Person am Computer auch berechtigt ist, diese vertraulichen Daten zu sehen. Nutzer werden also beim Zugriff aufs Dashboard ein weiteres Mal nach ihrem Passwort gefragt, selbst wenn sie bereits mit ihrem Google Account angemeldet sind. Auch reagierten wir auf den Nutzerwunsch nach Hilfe und Unterstützung: Googles „Gut zu Wissen"-Kampagne bietet viel Information und Tipps dazu, wie man sich sicher im Internet bewegt, was ein starkes Passwort ausmacht, was Cookies sind und wie sie funktionieren, wie man anhand der Internetadresse (IP) den Ort bestimmt, was Google genau an Daten speichert, wie man das Webprotokoll löschen kann und vieles mehr.

Nicht immer aber ist der Schritt von den Erkenntnissen zur Maßnahme so geradlinig wie in diesen Beispielen. Viel häufiger müssen wir uns in unserer Arbeit die Frage stellen, was eigentlich „gute Privacy UX" ausmacht, d. h. wie man diesen Aspekt der Nutzungserfahrung messen und bewerten kann.

4. Die Forschungsergebnisse ins Design übersetzen: Privacy UX Design

4.1. Die Qualität der datenschutzbezogenen Nutzungserfahrung messbar machen

Typische Qualitätskriterien für Interaktionsdesign fokussieren (natürlich) primär auf Usability (z. B. ISO-Kriterien) und manchmal zusätzlich auf hedonische Aspekte der Nutzung (Hassenzahl et al., 2000). Gängige Instrumente basieren auf der ISO 9241-10 (z. B. Gediga, Hamborg & Düntsch, 1999). Der AttrakDiff (Hassenzahl et al., 2003) erstellt aus pragmatischen und hedonischen Qualitäten eine Gesamtqualität. Heuristiken wie die von Nielsen (1993) oder Tognazzini (2003) geben Leitschnüre für „gutes", gebrauchstaugliches Design. Darüber hinaus werden Metriken verwendet wie Task Completion Rate oder Task Completion Time.

Für den Anteil „datenschutzbezogene Nutzungserfahrung" von Privacy UX bestehen keine derartigen Instrumente oder Heuristiken. Das hat mehrere Gründe:

- „Datenschutz" oder „Privacy" ist schwer zu definieren und noch schwerer zu messen. Gemessen (oder erforscht) werden können meist Datenschutzbedenken, die dann aber durch stark davon abweichendes beobachtbares Verhalten wieder relativiert werden (z. B. Buchanan et al., 2007). Es gibt also eine Diskrepanz zwischen Einstellung und Verhalten.
- Es bestehen große interkulturelle Unterschiede darin, was Regulatoren und Juristen unter „Privacy" verstehen und was durch „Privacy" geschützt werden soll. Beispielsweise gibt es in den USA die Auffassung von Privacy als „Right to be left alone", die auf die US-Verfassung zurückgeführt wird (Warren & Brandeis, 1890). In Deutschland leitete das Bundesverfassungsgericht 1983 im „Volkszählungsurteil" das Recht auf informationelle Selbstbestimmung vom Allgemeinen Persönlichkeitsrecht (Art. 2 GG) ab.

Wir mussten also unsere eigenen Kriterien ableiten.

4.2. Kriterien für eine gute Nutzungserfahrung aus Sicht von Privacy UX definieren

Um zu empirisch abgeleiteten und nützlichen Kriterien nach einem Fragenkatalog-Prinzip zu gelangen, gingen wir wie folgt vor:

Zunächst generierten wir bei einem erneuten Durchgang aller UPOP-Erkenntnisse pro Erkenntnis Bündel von Fragen, die auf diese spezifische Erkenntnis abzielten. Beispielsweise ergab unsere UPOP-Erkenntnis „Kein verlässliches Feedback" die Frage: „Werden Lösungen mit Feedback und zusätzlicher Information angeboten (insbesondere für den Fall, dass im Bereich des Datenschutzes

etwas schief läuft)?“ Dies ergab ca. 70 Fragen. Anschließend filterten wir die 70 Fragen auf Redundanzen und gruppierten sie letztlich in sieben einigermaßen trennscharfe Cluster (z. B.: „Contextual guidance & problem-solving“). Abschließend erbrachte ein erneuter (intuitiver) Kondensations- und Filterdurchgang zwölf (z.T. umformulierte) Fragen in drei Clustern: „User Control & Feedback“, „Privacy User Education“ sowie „Privacy Guidelines & Beyond“.

4.3. Privacy UX-Qualitätskriterien

Die oben beschriebene Vorgehensweise ermöglichte es uns, aus den UPOP-Ergebnissen die folgenden Kriterien abzuleiten:

Steuerbarkeit durch den Nutzer und Feedback (User Control and Feedback):
- Können die Nutzer die Kontrolle über ihre Daten ergreifen und ausüben?
- Wie werden Prozesse den Nutzern gegenüber kommuniziert und erklärt, insbesondere solche, die den Umgang mit ihren Daten betreffen?
- Werden Lösungen mit Feedback und zusätzlicher Information angeboten (insbesondere für den Fall, dass im Bereich des Datenschutzes etwas schief läuft)?
- Wie geht das Produkt mit mehreren Nutzern und / oder mehreren Geräten um?

Datenschutzbezogene Nutzerinstruktion (Privacy User Education):
- Wie wird den Nutzern erklärt, wie das Produkt mit ihren Daten umgeht / was es mit ihren Daten tut?
- Wie wird auf die unterschiedlichen Lernstile und Kenntnisstände über private / vertrauliche Daten eingegangen?
- Werden Nutzern Strategien für ein „sicheres“ Online-Leben angeboten?

Datenschutzregelwerke und darüber hinaus (Privacy Guidelines and Beyond):
- Wie wird über die Datensicherheits-Standards hinaus dafür gesorgt, dass Nutzer ihre Daten dem Produkt und Google anvertrauen?
- Wie sehen die Vorkehrungen für den Fall aus, dass es zu einem Datenschutz-Leck kommt (von Google oder den Nutzern verursacht)?
- Wie werden interne und externe Regelwerke und „Best Practices“ im Interesse der Nutzer verwendet?
- Wie wird festgestellt, dass das Standardverhalten des Produkts auch „gutes“ Standardverhalten für die Nutzer darstellt?

Diese neuen Kriterien und ein kleines Set von UI-Patterns werden zurzeit einem Praxistest unterzogen: Wir werden sie als Richtschnur in UI- und Konzept-Reviews für eigene und fremde Projekte anzuwenden versuchen und dabei beobachten, wie gut sie uns helfen, die Nutzer-Perspektive auf Datenschutz noch besser zu vertreten. Auch arbeiten wir daran, alle Mitglieder des Teams auf vergleichbare Privacy UX-Maßstäbe hin zu kalibrieren, um verlässlichere Ergebnisse aus Privacy UI-Reviews zu bekommen. Mittelfristig erhoffen wir uns, die Fragen noch stärker standardisieren und in ein Regelwerk überführen zu können, so dass andere Produktteams den Datenschutz noch stärker im Design berücksichtigen können.

5. Lessons learned: Wie wir Privacy UX bei Google etablieren konnten

Wie ist es uns gelungen, Privacy UX innerhalb der Firma erfolgreich zu etablieren? Die folgenden Faktoren waren aus unserer Sicht hilfreich:
- Privacy muss ganz tief in der Unternehmenskultur verankert sein oder werden. Das ist erstaunlicherweise möglich, selbst wenn die Firma schon mehr als zehn Jahre besteht. Eine mit entsprechenden Befugnissen und Ressourcen ausgestattete Stelle zu schaffen, erwies sich dabei als zentral. Bei Google wurde dazu die Position eines Director of Privacy, Product & Engineering geschaffen.
- Unterstützung „von ganz oben“ ist notwendig: Privacy in der Produktentwicklung konkret zu berücksichtigen, ist ein Quartals- und Jahresziel für jedes Entwicklungsteam. Die Teams müssen ihre Produktneuerungen einem Privacy Review-Prozess unterziehen. Im Rahmen dieses Prozesses beurteilt eine Gruppe von interdisziplinären Privacy-Experten das Produktkonzept und teilweise auch die Ausführung und gibt Rückmeldung, die für das Produkt sehr weitreichend sein können.
- Privacy ist nicht primär ein Security-, sondern ein Nutzerthema: Es geht hier um Vertrauen, das besonders im Web-Umfeld so wichtig ist, weil „der Wettbewerb nur einen Mausklick entfernt“ ist. Mit dem Thema Privacy kann man Wettbewerbsvorteile gewinnen: Nutzer vertrauen den Produkten und der Marke mehr, wenn wir ihnen Transparenz, Kontrolle und sinnvolle Wahlmöglichkeiten geben.
- Ein verlässliches Netzwerk mit anderen (senioren) UX-Leuten innerhalb der Firma ist hilfreich: Gerade Privacy UX-Arbeit geht stärker über Produktgrenzen hinweg als irgendein anderer Aspekt von UX.
- Wie für alle UX-Positionen, gilt auch für Privacy UX: Man sollte vermeiden, sich in die Rolle der Design-Polizei zu begeben. Stattdessen muss man darauf hinarbeiten, als hilfreich für andere Teams wahrgenommen zu werden.

Literatur

1. Buchanan, T., Paine, C., Joinson, A. N. & Reips, U.-D. (2007). Development of measures of online privacy concerns and protection for use on the Internet. Journal of the American Society for Information Science and Technology, 58(2), S. 157-165.
2. Fishbein, M. & Aijzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley.
3. Gediga, G., Hamborg, K.-C. & Düntsch, I. (1999). The IsoMetrics usability inventory:

An operationalisation of ISO 9241-10. Behaviour and Information Technology, 18, S. 151-164. http://www.isometrics.uni-osnabrueck.de/paper/bit.htm – letzter Zugriff am 26.6.2012
4. Hassenzahl, M., Platz, A., Burmester, M. & Lehner, K. (2000). Hedonic and ergonomic quality aspects determine a software's appeal. In: Proceedings of the CHI 2000 Conference on Human Factors in Computing, Den Haag, S. 201-208.
5. Hassenzahl, M., Burmester, M. & Koller, F. (2003). AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In G. Szwillus, J. Ziegler (Hrsg.): Mensch & Computer 2003: Interaktion in Bewegung. Stuttgart: B. G. Teubner, S. 187-196.
6. Joinson, A., Reips, U.D., Buchanan, T., & Paine Schofield, C. B. (2010). Privacy, trust and self-disclosure online. Human Computer Interaction, 2010, Volume 25, S. 1-24.
7. Nielsen, J. (1993). Usability Engineering. San Francisco, CA: Morgan Kaufmann Publishers.
8. Ortlieb, M. (2011). Global Differences in Perceptions of Privacy. Präsentation auf der Konferenz „Privacy, Identity, Innovation 2011" im Silicon Valley am 20.5. 2011. http://www.privacyidentityinnovation.com/events/pii2011-silicon-valley – letzter Zugriff am 26.6.2012.
9. Ortlieb, M. (2011). Unclear social etiquette online: how users experiment (and struggle) with interacting across many channels and devices in an ever-evolving and fast-changing landscape of communication tools. In Ethnographic Praxis in Industry Conference Proceedings, Volume 2011 (1), S. 311-321.
10. Tognazzini, B. (2003). First Principles of Interaction Design. http://www.asktog.com/basics/firstPrinciples.html – letzter Zugriff am 26.6.2012
11. Warren, S. D. & Brandeis, L. D.: The right to privacy. Harward Law Review, Vol. IV, No. 5. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html – letzter Zugriff am 25.7.2012
12. EU Datenschutz-Vorordnung (Entwurf): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf – letzter Zugriff am 26.6.2012
13. E-Privacy-Direktive: circumstances, procedures and formats for personal data breach notifications: http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/data_breach/ePrivacy_databreach_consultation.pdf – letzter Zugriff am 26.6.2012.