Ask 100 people if they care for privacy and 85 will say yes.
Ask those same 100 people if they'll give you a DNA sample just to get a free Big Mac, and 85 will say yes.

— Austin Hill (Zero-Knowledge Systems), 2002

Zielkonflikte in Usability und Privacy

Dr. Dominik Herrmann

Folien: https://dhgo.to/slides-zielkonflikte

Privacy-Paradoxon

Ask 100 people if they care for privacy and 85 will say yes.
Ask those same 100 people if they'll give you a DNA sample
just to get a free Big Mac, and 85 will say yes.

— Austin Hill (Zero-Knowledge Systems), 2002

Zielkonflikte in Usability und Privacy

Gliederung

1. **Usability und Privacy**
2. Fallstudie: Tools zum Schutz vor Tracking im Internet
3. Fallstudie: elektronische Evaluation von Vorlesungen

Ziel der Vorlesungseinheit:

- Sie können Zielkonflikte anhand eines Beispiels erläutern.
- Sie können an einem Beispiel erläutern, wie sich Zielkonflikte durch datenschutzfreundliche Techniken auflösen lassen.

Usability hat zahlreiche Facetten und Bezüge zu anderen Disziplinen.

Usability ist eine **nichtfunktionale Qualitätsanforderung** an Anwendungs- und Informationssysteme.

weitere nicht-funktionale Anforderungen: Skalierbarkeit, Wartbarkeit, Sicherheit, …

Kriterien für Usability (ISO 9241-11)
Effektivität, Effizienz, Zufriedenheit
(in einem definierten Kontext)

andere Kriterien z.B. bei Nielsen (2012): **efficiency, satisfaction, learnability, memorability, errors**

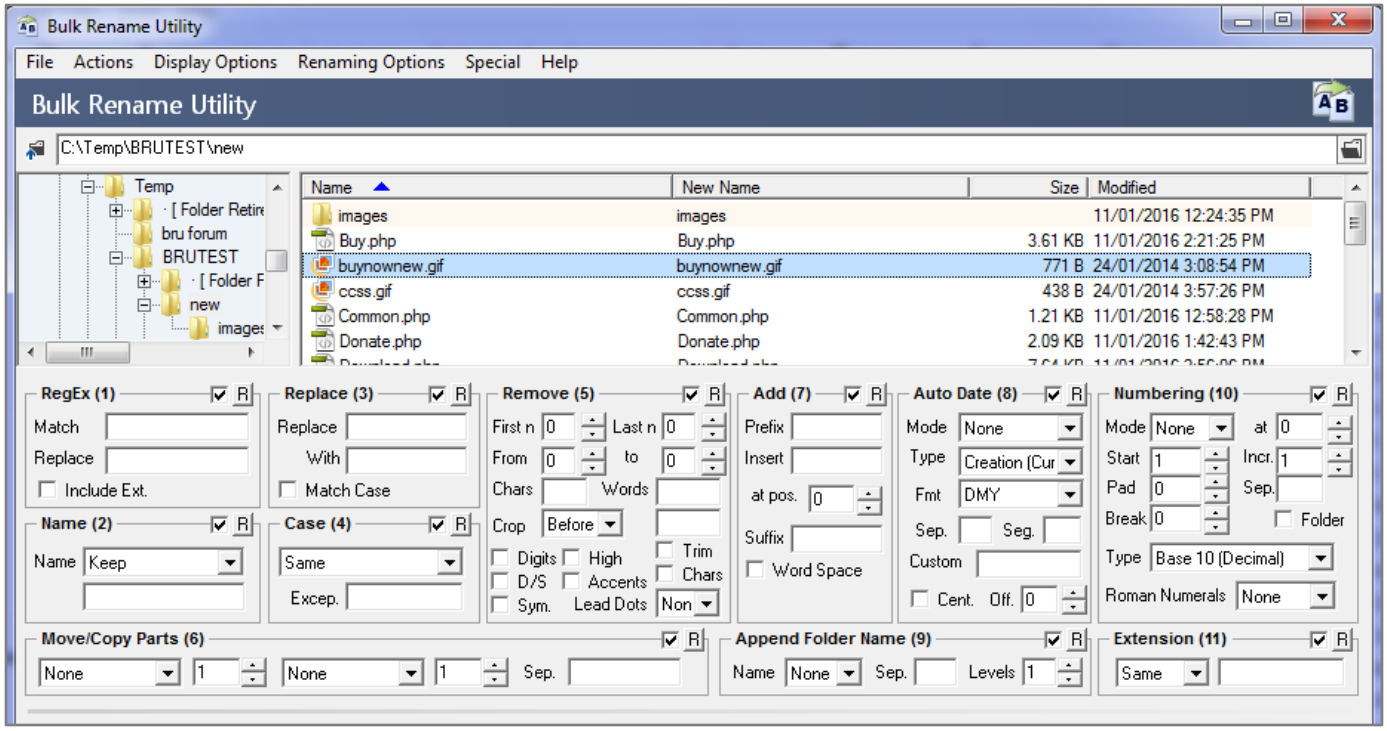
Bezüge zu anderen Disziplinen
- Mensch-Computer-Interaktion (MCI)
- (Wirtschafts-)Informatik
- (Verhaltens-)Psychologie
- User Experience (UX)

Usability ist **mehr als gutes Design**; berücksichtigt auch die Nützlichkeit.

pinterest.com/pin/44684221275192053/

K. Adams (2015): Non-functional Requirements in Systems Analysis and Design, Springer.
https://www.nngroup.com/articles/usability-101-introduction-to-usability/

Es gibt zahlreiche Usability-Methoden für den Entwurf und für die Evaluation.



www.bulkrenameutility.co.uk

Entwurf

Prototyping
Personas
nutzerzentriertes Design

Evaluation

Cognitive Walkthroughs
Befragung von Nutzern
Feld- und Laborstudien

Auch Privacy hat zahlreiche Facetten und Bezüge zu anderen Disziplinen.

Privacy bezieht sich auf den **Schutz der Privatsphäre** (Menschenrecht).

Privacy in Informationssystemen:
Fokus auf Schutz der **personen-bezogenen Daten**

Privatsphäre kann aufgegeben oder eingeschränkt werden (z.B. zur Strafverfolgung)

Bezüge zu anderen Disziplinen
- (Datenschutz-)Recht
- (Wirtschafts-)Informatik
- (Verhaltens-)Psychologie
- Philosophie und Ethik

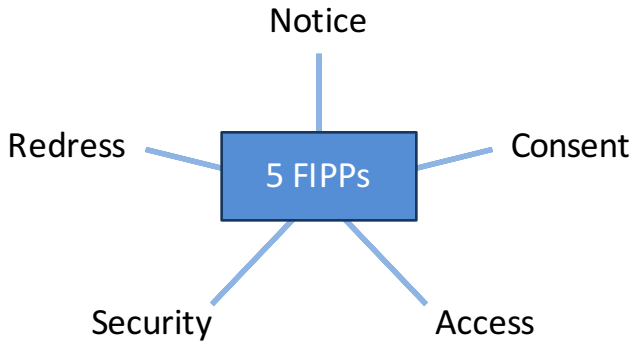
Privatsphäre: nicht-öffentlicher Bereich, in dem ein Mensch seine Persönlichkeit frei entfalten kann.

Recht auf informationelle Selbstbestimmung (1983)

Bezug zur Informationssicherheit: **Vertraulichkeit**

Privacy-Prinzipien und ihre Umsetzung

1970: Hessisches Datenschutzgesetz
1980: OECD Guidelines
1995: EU Data Protection Directive
1998: FTC **Fair Information Practice Principles** (FIPP)
2018: EU General Data Protection Regulation (2018)

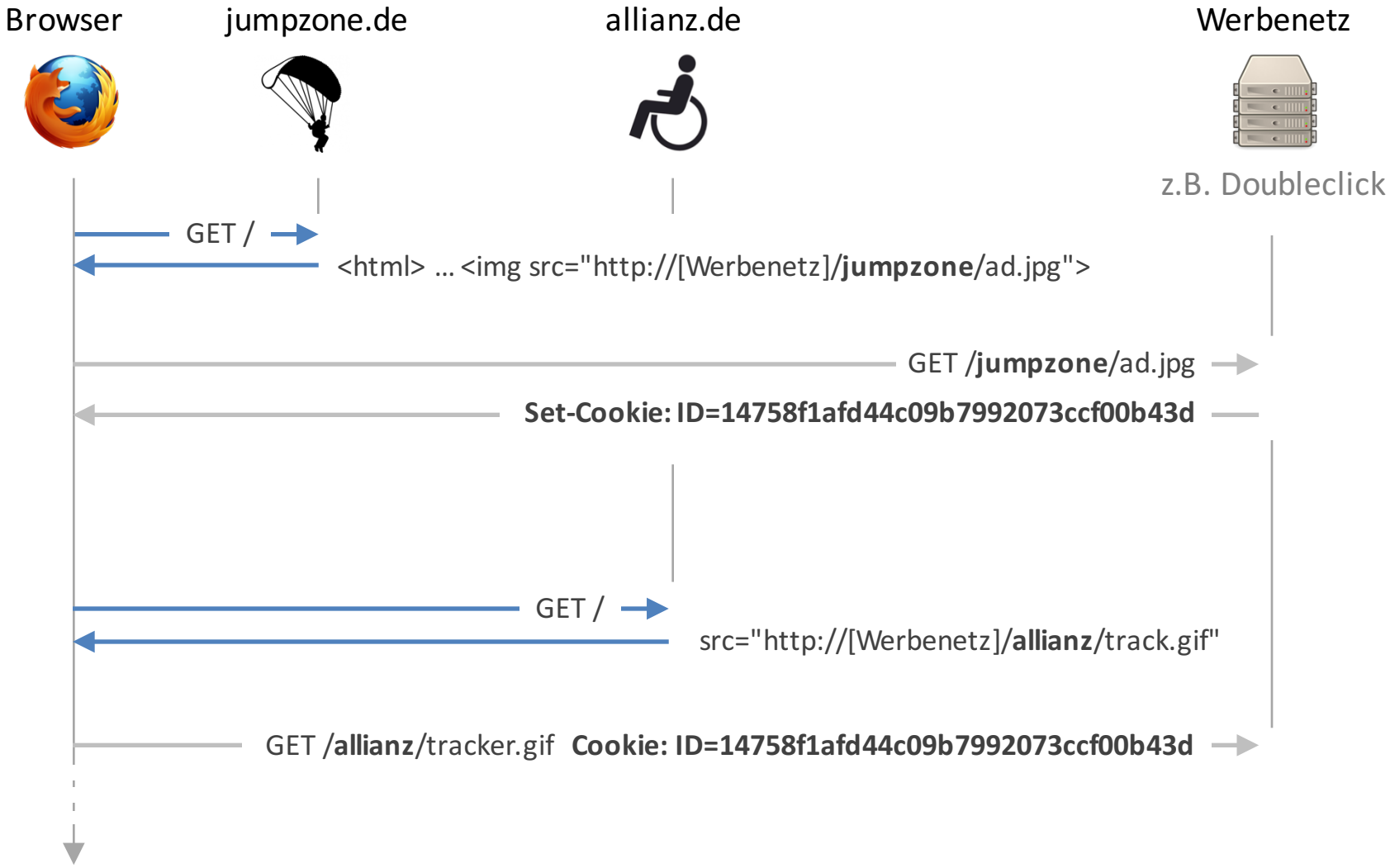


D. J. Solove (2008): Understanding Privacy, Harvard University Press.

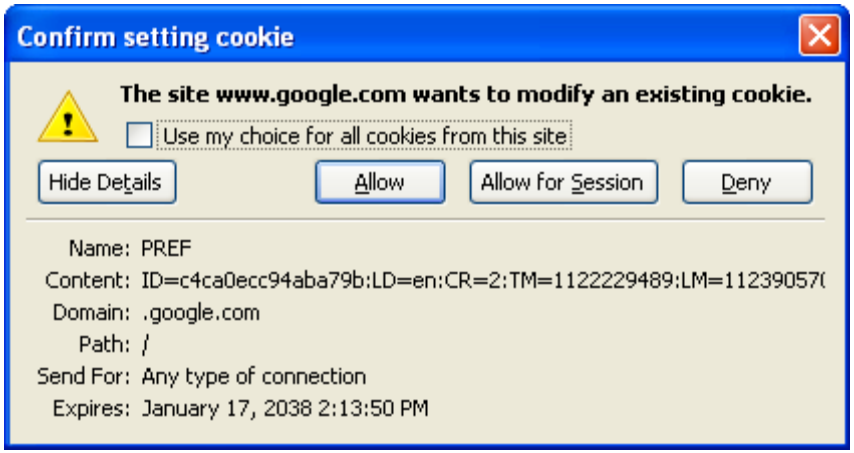
Gliederung

1. Usability und Privacy
2. **Fallstudie: Tools zum Schutz vor Tracking im Internet**
3. Fallstudie: elektronische Evaluation von Vorlesungen

Trackingdienste verfolgen die Aktivitäten von Internetnutzern über Seitengrenzen hinweg.



Zielkonflikt 1: Streben nach Usability (*Effizienz, ease of use*) geht zu Lasten von Privacy (notice, control) in der Standardkonfiguration.



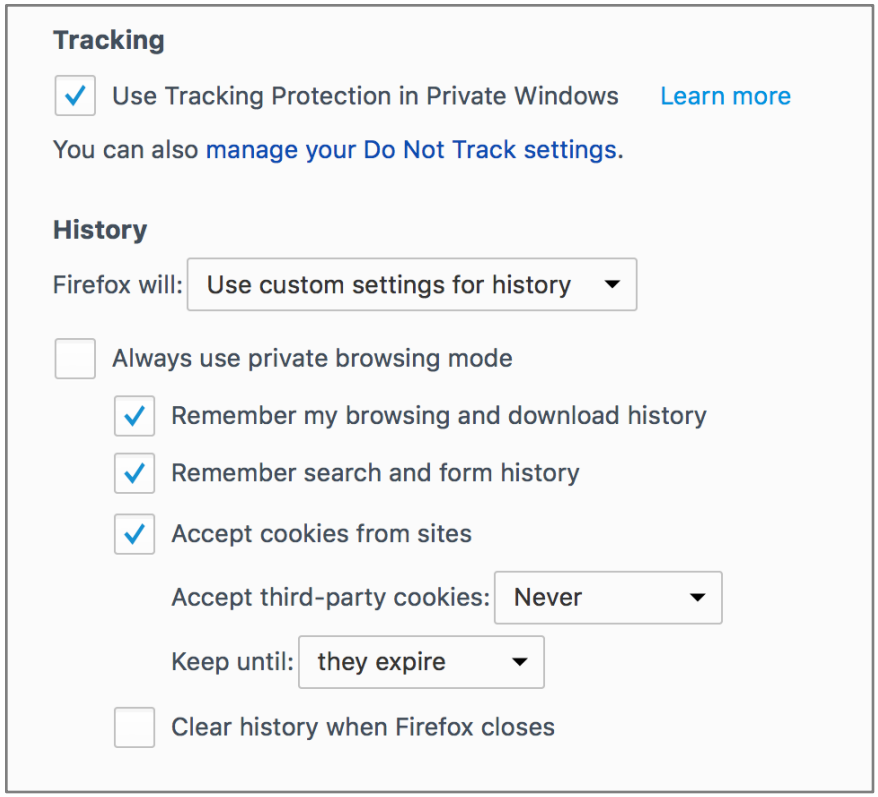
immer mehr Seiten nutzen First-Party-Cookies

Browser fragen bei jedem Cookie, ob es gespeichert werden soll

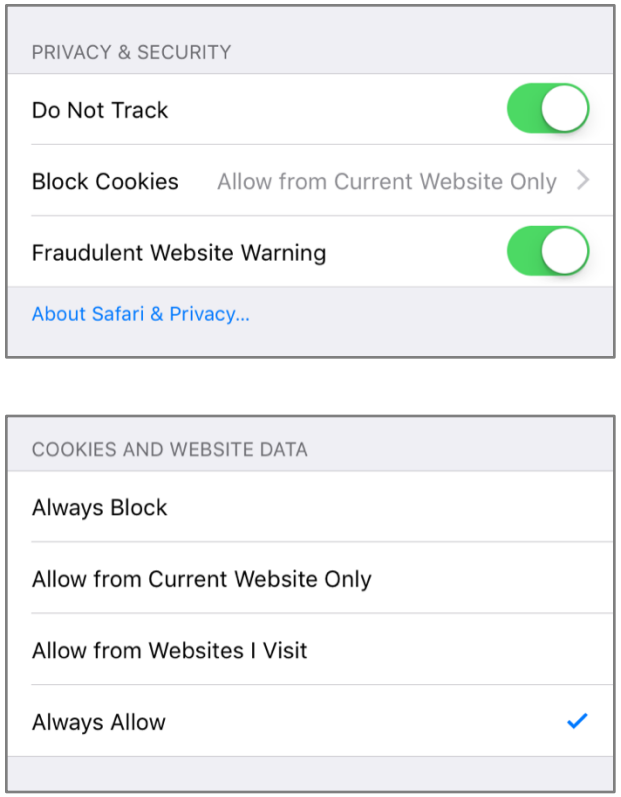
immer mehr Seiten nutzen Tracking-Dienste mit Third-Party-Cookies

Browser akzeptieren im Auslieferungszustand alle Cookies.

Zielkonflikt 2: Unzureichende Usability und Privacy sind Folge des Bestrebens, mit *einer* Benutzerschnittstelle Anfänger *und* Experten zu adressieren.



Firefox 34



iOS 10

Hürden: Bedeutung unklar | Konsequenzen unklar | beste Wahl unklar

Gabrielli & Jameson (2009): Obstacles to Option Setting: Initial Results With a Heuristic Walkthrough Method. INTERACT 2009, p. 600–603.

Software-Entwickler nutzen unglückliche Metaphern, weshalb die „Mental Models“ der Anwender nicht der Realität entsprechen.

Ungeeignete Metapher: **Cookies**, die **im Browser abgelegt** werden.

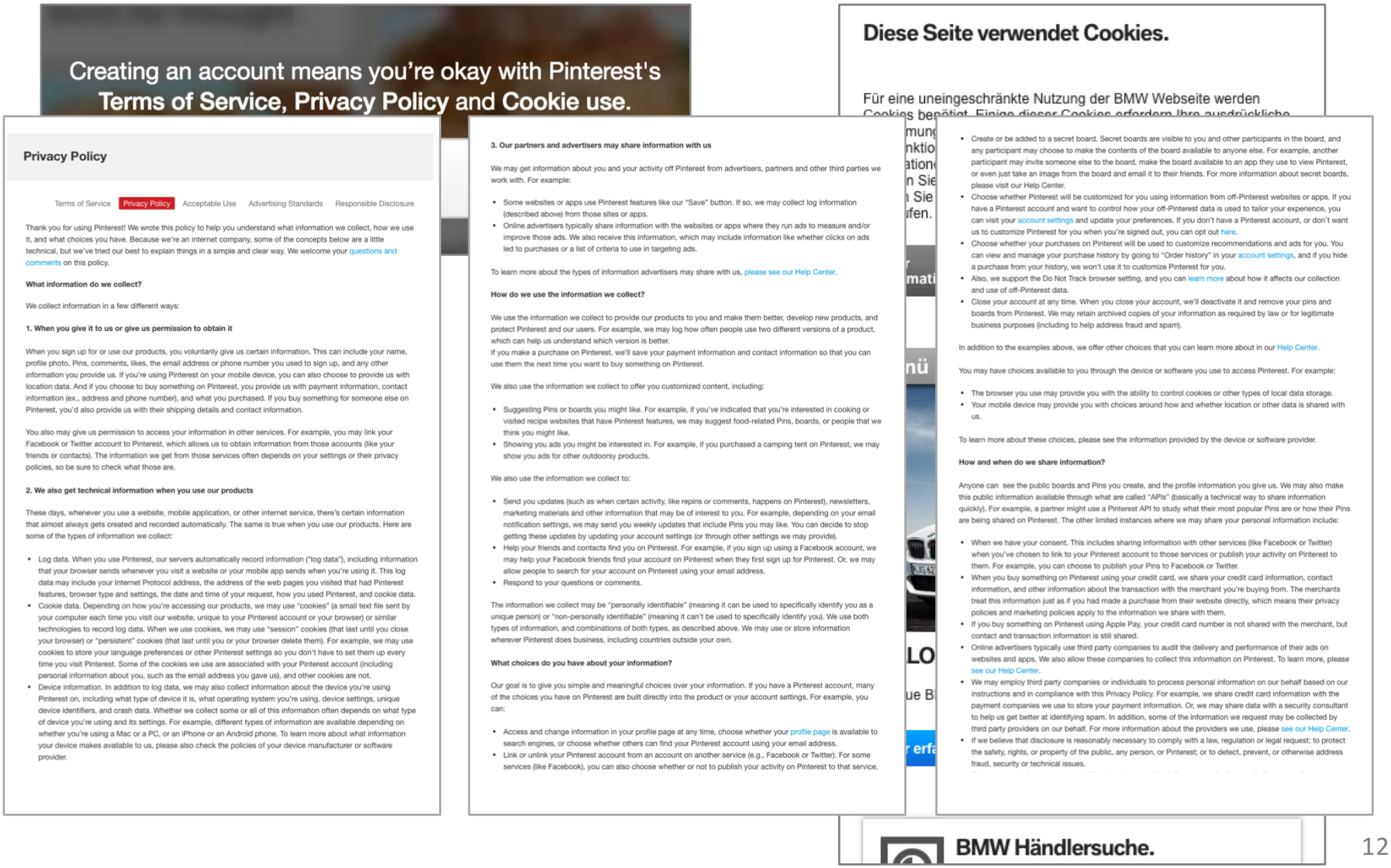
Das Ablegen ist nicht schlimm – das spätere Übermitteln im Kontext einer anderen Webseite hingegen schon.

Bessere Metapher: **Barcode-Label**

Der Browser wird mit einem Barcode markiert, der beim Besuch jeder Webseite erfasst und an eine Auswertungszentrale übermittelt wird.

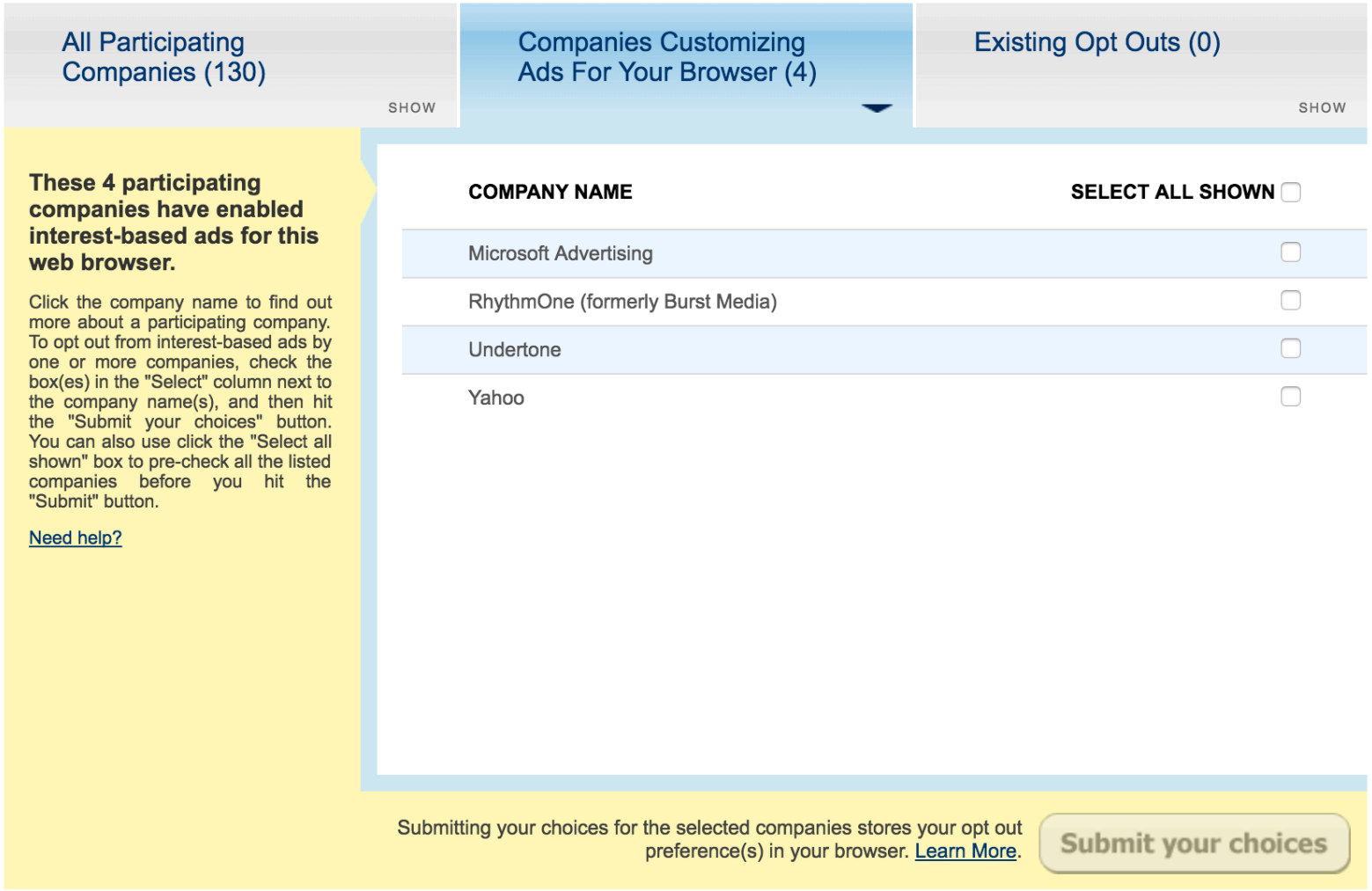
Zielkonflikt 3: Usability vs. rechtliche Anforderungen (notice & consent)

Umsetzung rechtlicher Auflagen resultiert in schlecht benutzbaren Lösungen

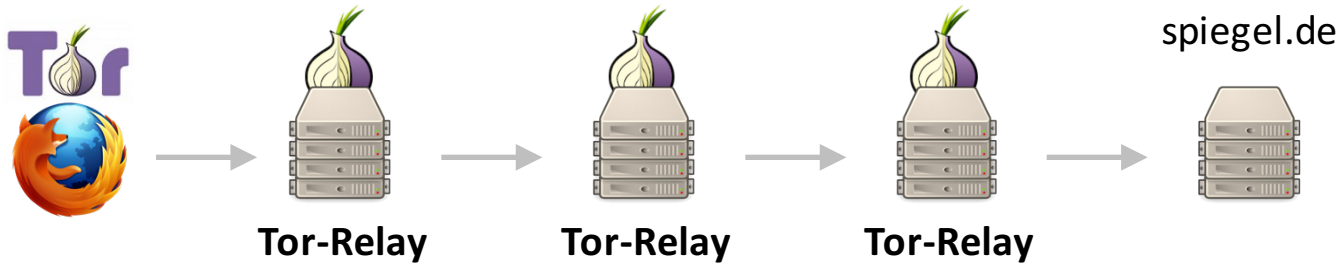


Zielkonflikt 4: Unterschiedliche Interessen von Anwendern und Dienstanbietern

vgl. Opt-Out-Cookies beeinträchtigen Privacy und Usability.

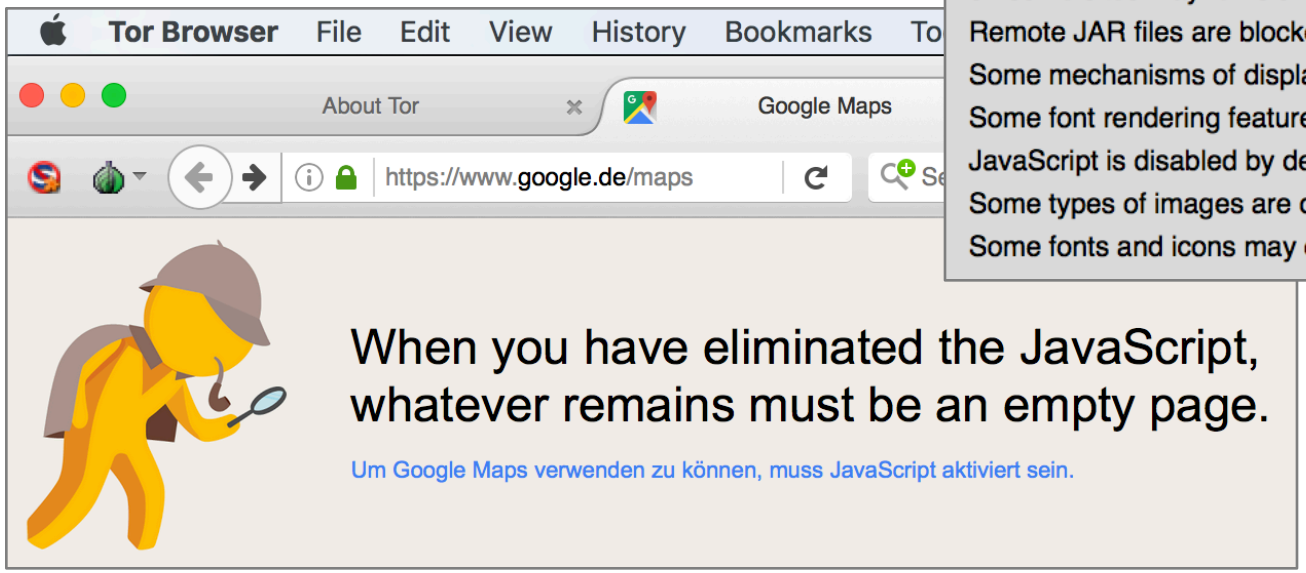


Zielkonflikt 5: Gängige Selbstdatenschutz-Tools erreichen Schutz der Privatsphäre auf Kosten der Usability, etwa weil gängige Dienste unbenutzbar sind.



Ladezeit (3G)	[s]
mit Tor:	13
ohne Tor:	40
ohne + Adblock:	4

!



Gliederung

1. Usability und Privacy
2. Fallstudie: Tools zum Schutz vor Tracking im Internet
3. **Fallstudie: elektronische Evaluation von Vorlesungen**

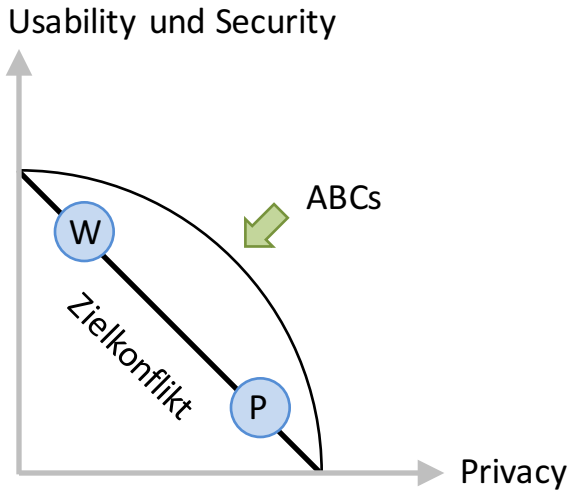
Bei der Evaluation von Lehrveranstaltungen gibt es Zielkonflikte zwischen Anonymität und Authentizität, die sich auf die Usability auswirken.

Papierbasierte Evaluation (P)

- hoher logistischer Aufwand
- Evaluation nicht an regelmäßige Kursteilnahme geknüpft

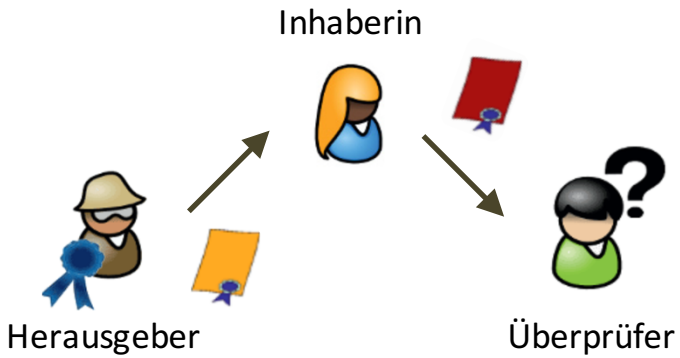
Webbasierte Evaluation (W)

- Vertrauen in Betreiber nötig



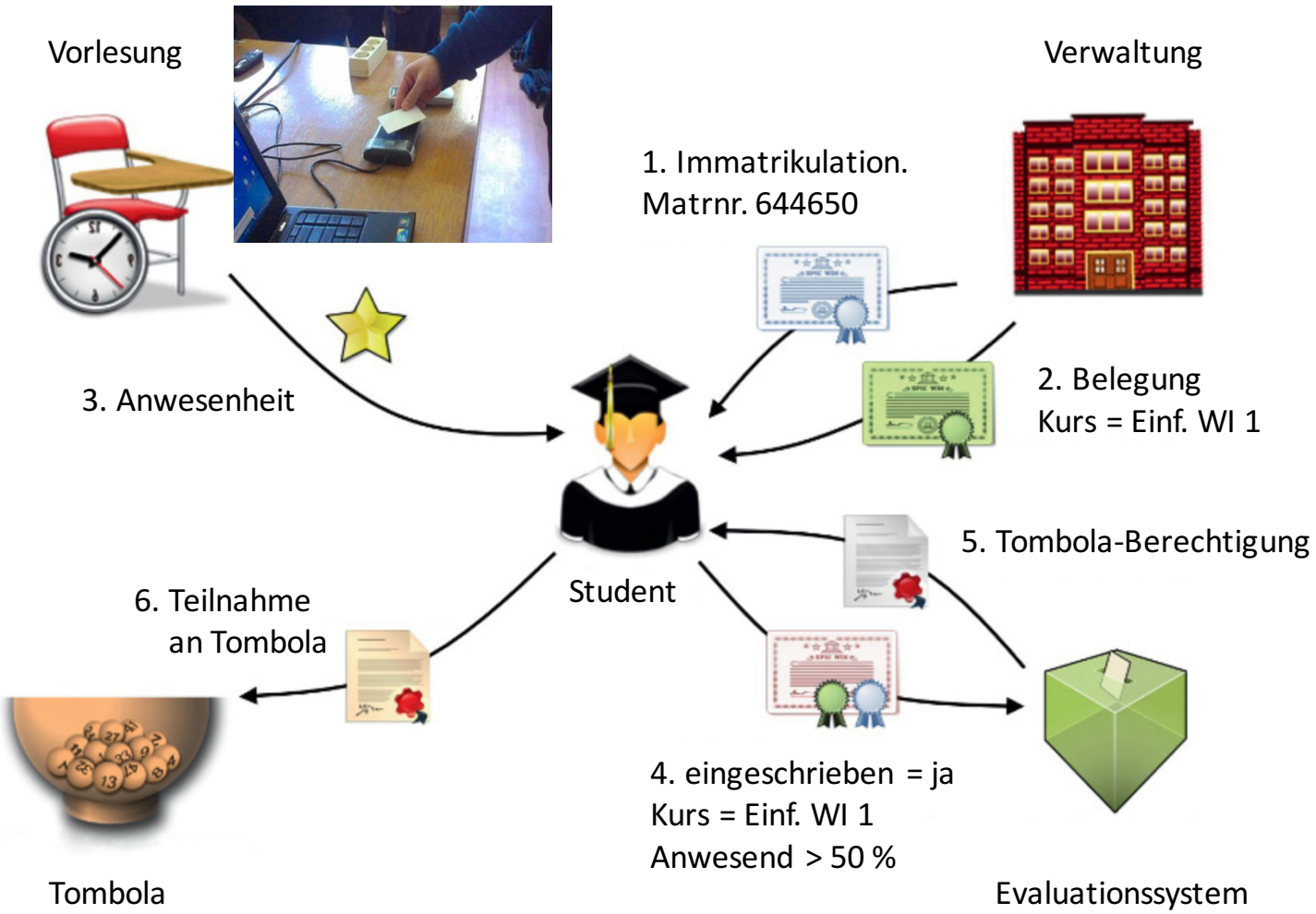
Attributbasierte Zertifikate (ABCs)

- **Pseudonymität** und **Unverkettbarkeit**
- ein Kurs kann **nur einmal evaluiert** werden
- Evaluation **setzt Immatrikulation** und **Teilnahme** an 50 % der Termine voraus



Mayer & Narayanan (2013): Privacy Substitutes. 66 Stanford Law Review 89.
Bichsel et al. (2015): An Architecture for Privacy-ABCs. In: Attribute-based Credentials for Trust, Springer.

An der Patras-Universität wurde ein Pilotprojekt durchgeführt, um die Nutzer-akzeptanz einer solchen Privacy-by-Design-Lösung zu untersuchen.

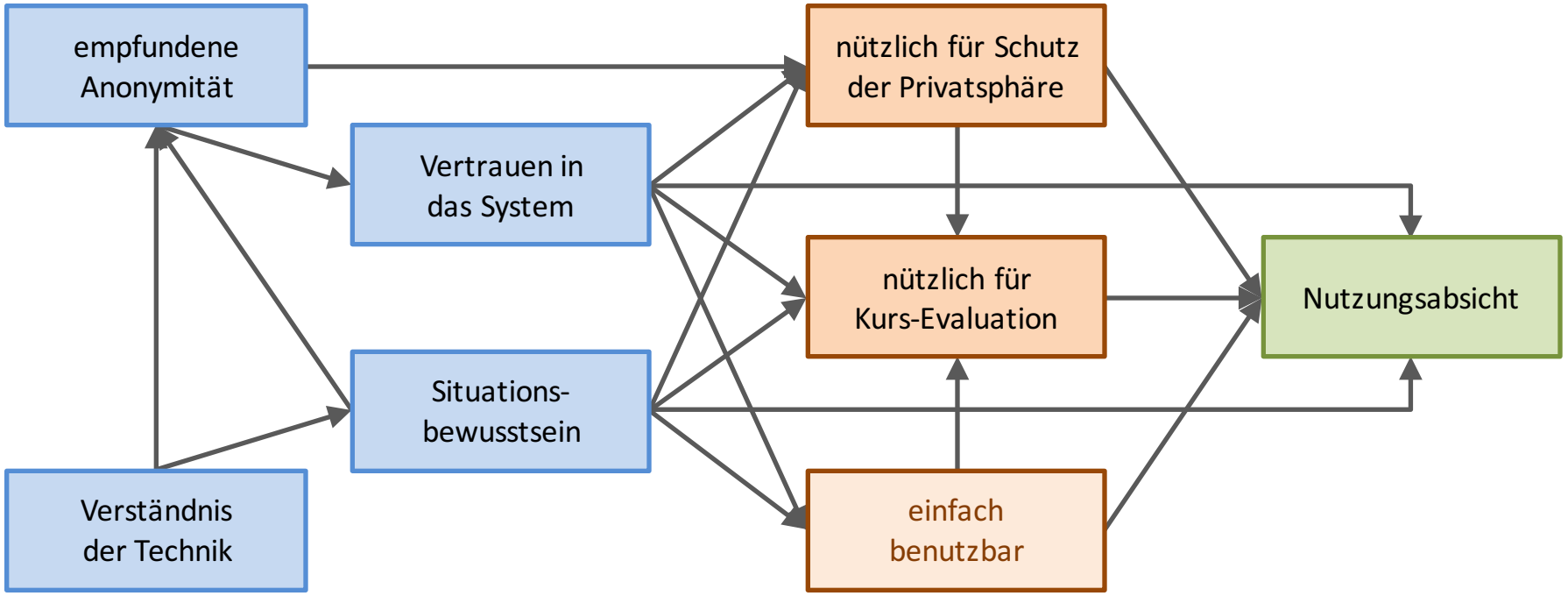


Stamatiou et al. (2015): Course Evaluation in Higher Education: the Patras Pilot of ABC4Trust. In: Attribute-based Credentials for Trust, Springer.

Nach einem Usability-Test wurden 30 Nutzer des Systems befragt, um Einflussfaktoren zu ermitteln, die für eine Nutzerakzeptanz wichtig sind.

29 fühlten sich anonym

Technology Acceptance Model



Nur 14 Nutzer wussten, dass ihre Matrikelnr. *nicht* an das System übermittelt wird.

28 Nutzer bevorzugten das System im Vergleich zur papierbasierten Evaluation.

vereinfachte Darstellung

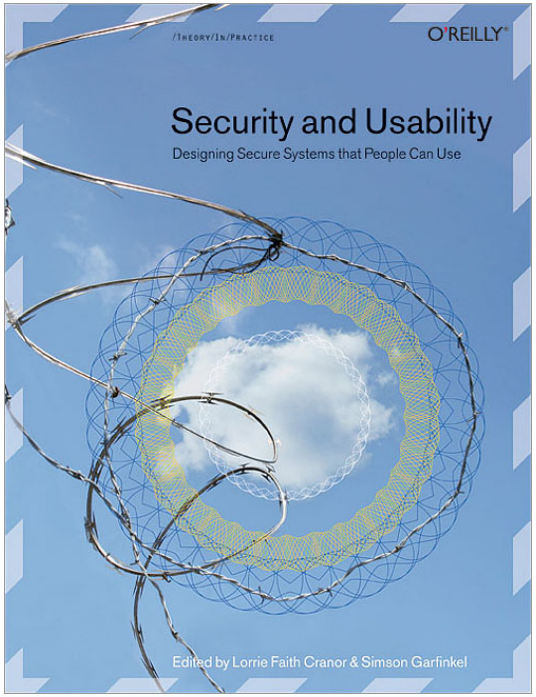
Stamatiou et al. (2015): Course Evaluation in Higher Education: the Patras Pilot of ABC4Trust. In: Attribute-based Credentials for Trust, Springer.

Zusammenfassung

Zwei Fallstudien
- Tools zum Schutz vor Tracking im Internet
- Elektronische Evaluation von Vorlesungen

Zielkonflikte in Usability und Privacy:
- restriktive **Standardkonfiguration** vs. Usability
- Bedürfnisse von **Anfängern und Experten**
- **rechtliche Anforderungen** vs. Usability
- gegensätzliche Ziele von **Anbietern und Nutzern**
- Unterstützung von Selbstdatenschutz-Tools vs. **Entwicklungsaufwand für die Anbieter**

Privacy by Design: Benutzbare und sichere Lösungen lassen sich realisie-ren, wenn Usability und Privacy bereits beim Entwurf berücksichtigt werden.



Cranor & Garfinkel (2014)