

*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.

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

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.

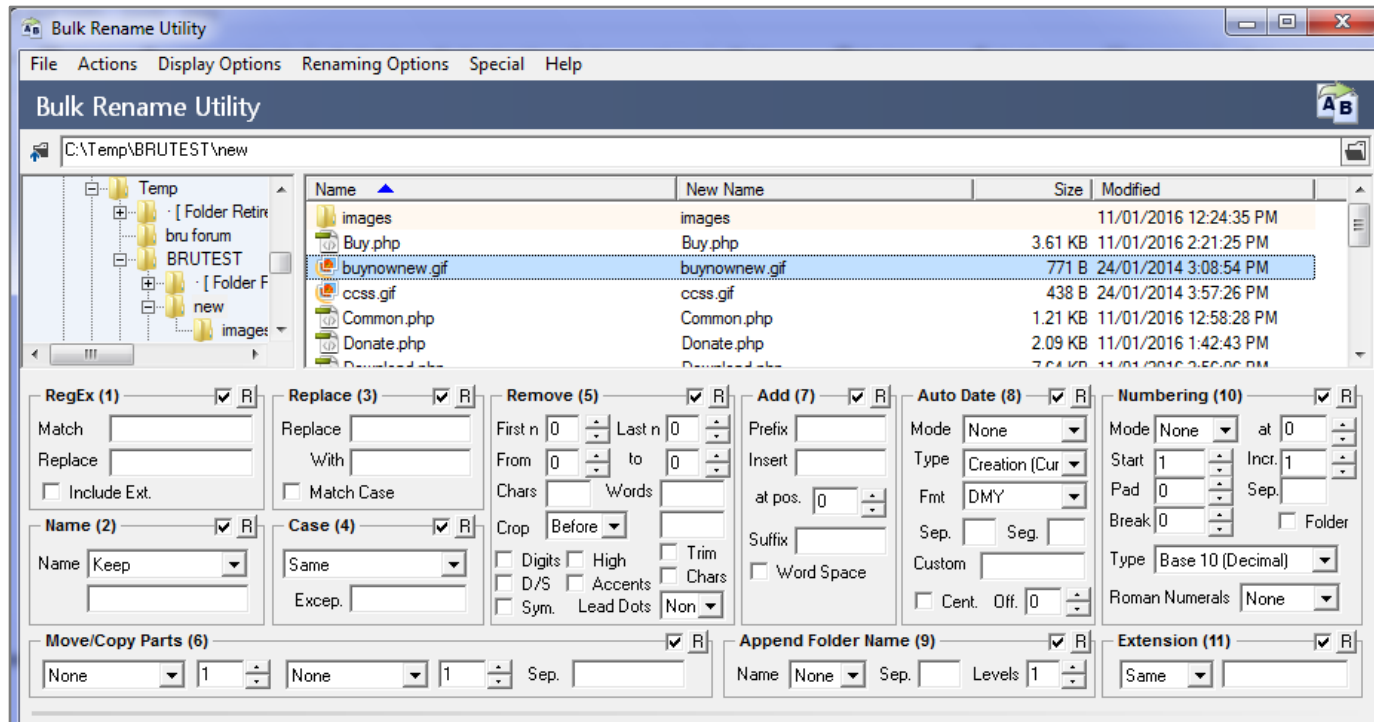
weitere nicht-funktionale Anforderungen:  
Skalierbarkeit, Wartbarkeit, Sicherheit, ...

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



[pinterest.com/pin/44684221275192053/](https://www.pinterest.com/pin/44684221275192053/)

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



[www.bulkrenameutility.co.uk](http://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 **personenbezogenen 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

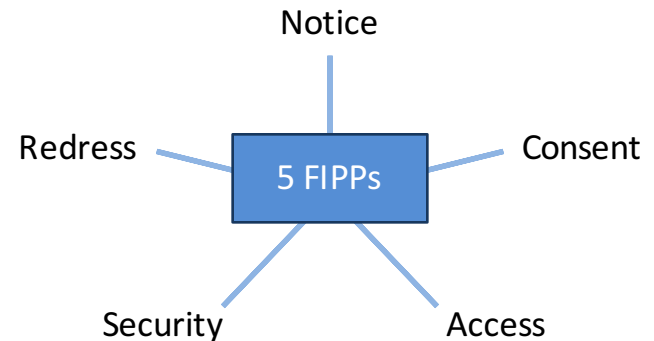
1970: Hessisches Datenschutzgesetz

1980: OECD Guidelines

1995: EU Data Protection Directive

1998: FTC **Fair Information Practice Principles** (FIPP)

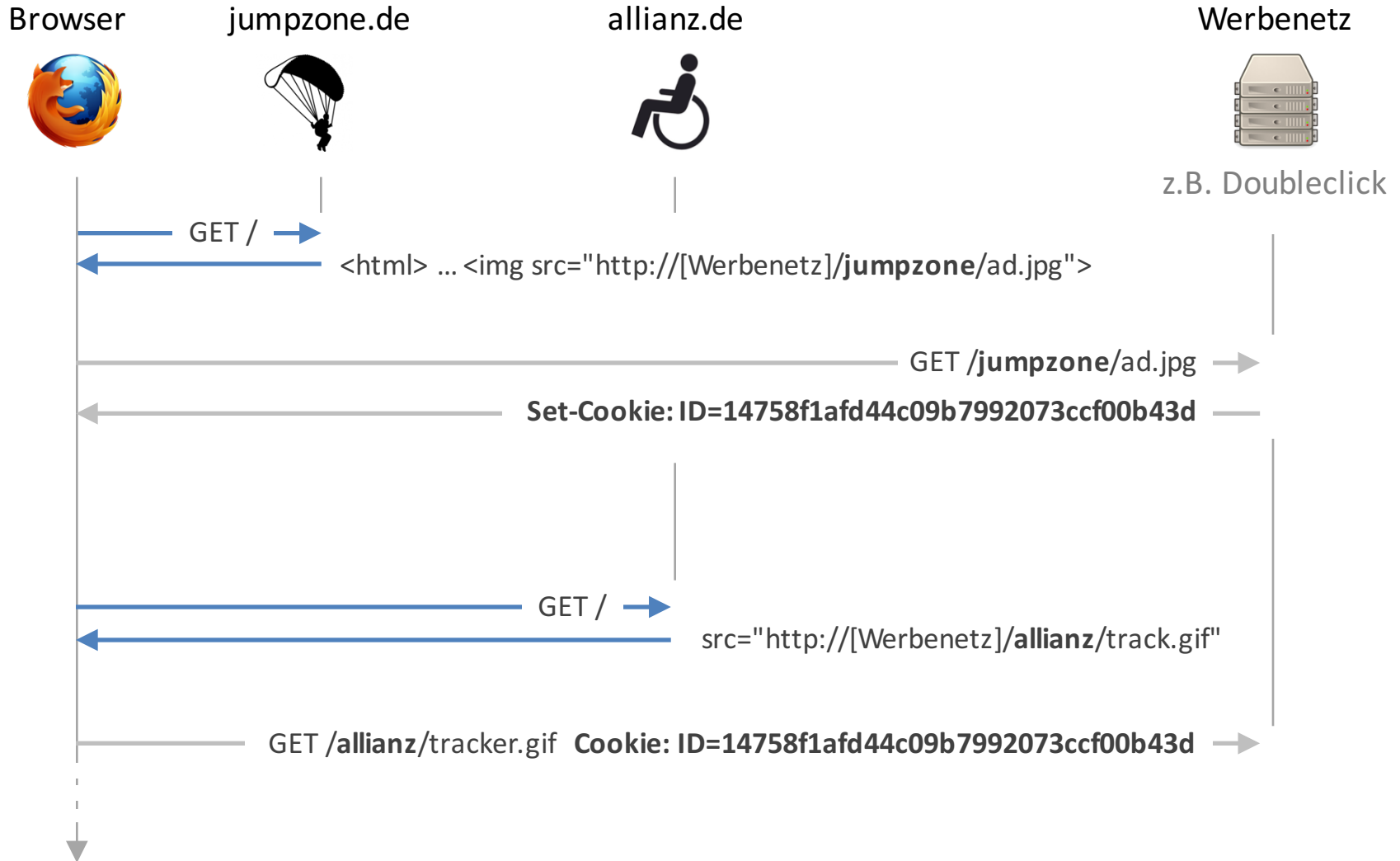
2018: EU General Data Protection Regulation (2018)



# Gliederung

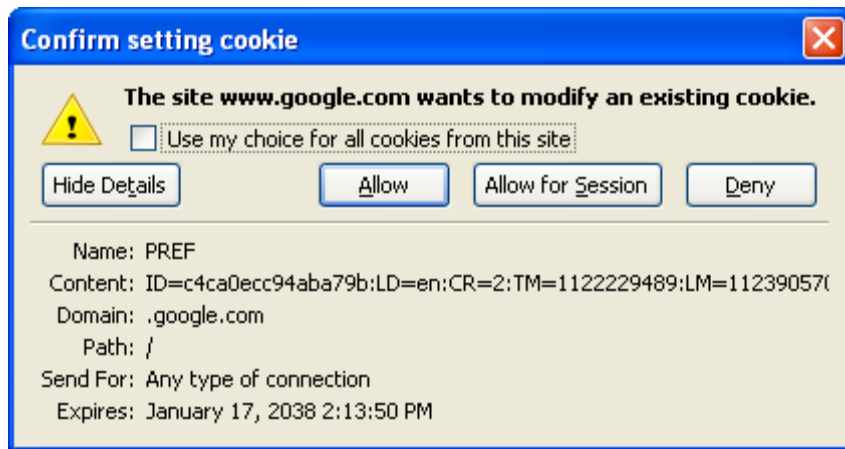
1. Usability und Privacy
2. **Fallstudie: Tools zum Schutz vor Tracking im Internet**
3. Fallstudie: elektronische Evaluation von Vorlesungen

# Trackingdienste verfolgen die Aktivitäten von Internetnutzern über Seitengrenzen hinweg.



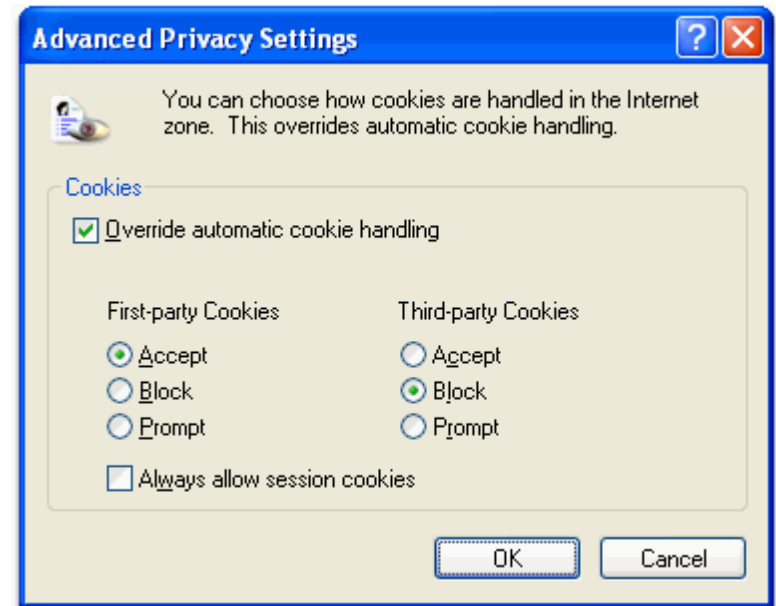


# Zielkonflikt 1: Streben nach Usability (*Effizienz, ease of use*) geht zu Lasten von Privacy (notice, control) in der Standardkonfiguration.



*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.

**Tracking**

Use Tracking Protection in Private Windows [Learn more](#)

You can also [manage your Do Not Track settings](#).

**History**

Firefox will:

Always use private browsing mode

Remember my browsing and download history

Remember search and form history

Accept cookies from sites

Accept third-party cookies:

Keep until:

Clear history when Firefox closes

Firefox 34

PRIVACY & SECURITY

Do Not Track

Block Cookies

Fraudulent Website Warning

[About Safari & Privacy...](#)

COOKIES AND WEBSITE DATA

Always Block

Allow from Current Website Only

Allow from Websites I Visit

Always Allow

iOS 10

Hürden:

Bedeutung unklar

Konsequenzen unklar

beste Wahl unklar

# 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

### Creating an account means you're okay with Pinterest's Terms of Service, Privacy Policy and Cookie use.

#### Privacy Policy

Terms of Service **Privacy Policy** Acceptable Use Advertising Standards Responsible Disclosure

Thank you for using Pinterest! We wrote this policy to help you understand what information we collect, how we use it, and what choices you have. Because we're an internet company, some of the concepts below are a little technical, but we've tried our best to explain things in a simple and clear way. We welcome your [questions and comments](#) on this policy.

#### What information do we collect?

We collect information in a few different ways:

##### 1. When you give it to us or give us permission to obtain it

When you sign up for or use our products, you voluntarily give us certain information. This can include your name, profile photo, Pins, comments, likes, the email address or phone number you used to sign up, and any other information you provide us. If you're using Pinterest on your mobile device, you can also choose to provide us with location data. And if you choose to buy something on Pinterest, you provide us with payment information, contact information (e.g., address and phone number), and what you purchased. If you buy something for someone else on Pinterest, you'd also provide us with their shipping details and contact information.

You also may give us permission to access your information in other services. For example, you may link your Facebook or Twitter account to Pinterest, which allows us to obtain information from those accounts (like your friends or contacts). The information we get from those services often depends on your settings or their privacy policies, so be sure to check what those are.

##### 2. We also get technical information when you use our products

These days, whenever you use a website, mobile application, or other internet service, there's certain information that almost always gets created and recorded automatically. The same is true when you use our products. Here are some of the types of information we collect:

- Log data. When you use Pinterest, our servers automatically record information ("log data"), including information that your browser sends whenever you visit a website or your mobile app sends when you're using it. This log data may include your Internet Protocol address, the address of the web pages you visited that had Pinterest features, browser type and settings, the date and time of your request, how you used Pinterest, and cookie data.
- Cookie data. Depending on how you're accessing our products, we may use "cookies" (a small text file sent by your computer each time you visit our website, unique to your Pinterest account or your browser) or similar technologies to record log data. When we use cookies, we may use "session" cookies (that last until you close your browser) or "persistent" cookies (that last until you or your browser delete them). For example, we may use cookies to store your language preferences or other Pinterest settings so you don't have to set them up every time you visit Pinterest. Some of the cookies we use are associated with your Pinterest account (including personal information about you, such as the email address you gave us), and other cookies are not.
- Device information. In addition to log data, we may also collect information about the device you're using Pinterest on, including what type of device it is, what operating system you're using, device settings, unique device identifiers, and crash data. Whether we collect some or all of this information often depends on what type of device you're using and its settings. For example, different types of information are available depending on whether you're using a Mac or a PC, or an iPhone or an Android phone. To learn more about what information your device makes available to us, please also check the policies of your device manufacturer or software provider.

#### 3. Our partners and advertisers may share information with us

We may get information about you and your activity off Pinterest from advertisers, partners and other third parties with work with. For example:

- Some websites or apps use Pinterest features like our "Save" button. If so, we may collect log information (described above) from those sites or apps.
- Online advertisers typically share information with the websites or apps where they run ads to measure and/or improve those ads. We also receive this information, which may include information like whether clicks on ads led to purchases or a list of criteria to use in targeting ads.

To learn more about the types of information advertisers may share with us, [please see our Help Center](#).

#### How do we use the information we collect?

We use the information we collect to provide our products to you and make them better, develop new products, and protect Pinterest and our users. For example, we may log how often people use two different versions of a product, which can help us understand which version is better.

If you make a purchase on Pinterest, we'll save your payment information and contact information so that you can use them the next time you want to buy something on Pinterest.

We also use the information we collect to offer you customized content, including:

- Suggesting Pins or boards you might like. For example, if you've indicated that you're interested in cooking or visited recipe websites that have Pinterest features, we may suggest food-related Pins, boards, or people that you think you might like.
- Showing you ads you might be interested in. For example, if you purchased a camping tent on Pinterest, we may show you ads for other outdoorsy products.

We also use the information we collect to:

- Send you updates (such as when certain activity, like repins or comments, happens on Pinterest), newsletters, marketing materials and other information that may be of interest to you. For example, depending on your email notification settings, we may send you weekly updates that include Pins you may like. You can decide to stop getting these updates by updating your account settings (or through other settings we may provide).
- Help your friends and contacts find you on Pinterest. For example, if you sign up using a Facebook account, we may help your Facebook friends find your account on Pinterest when they first sign up for Pinterest. Or, we may allow people to search for your account on Pinterest using your email address.
- Respond to your questions or comments.

The information we collect may be "personally identifiable" (meaning it can be used to specifically identify you as a unique person) or "non-personally identifiable" (meaning it can't be used to specifically identify you). We use both types of information, and combinations of both types, as described above. We may use or store information wherever Pinterest does business, including countries outside your own.

#### What choices do you have about your information?

Our goal is to give you simple and meaningful choices over your information. If you have a Pinterest account, many of the choices you have on Pinterest are built directly into the product or your account settings. For example, you can:

- Access and change information in your profile page at any time, choose whether your [profile page](#) is available to search engines, or choose whether others can find your Pinterest account using your email address.
- Link or unlink your Pinterest account from an account on another service (e.g., Facebook or Twitter). For some services (like Facebook), you can also choose whether or not to publish your activity on Pinterest to that service.

### Diese Seite verwendet Cookies.

Für eine uneingeschränkte Nutzung der BMW Webseite werden Cookies benötigt. Einige dieser Cookies erfordern Ihre ausdrückliche

- Create or be added to a secret board. Secret boards are visible to you and other participants in the board, and any participant may choose to make the contents of the board available to anyone else. For example, another participant may invite someone else to the board, make the board available to an app they use to view Pinterest, or even just take an image from the board and email it to their friends. For more information about secret boards, please visit our [Help Center](#).
- Choose whether Pinterest will be customized for you using information from off-Pinterest websites or apps. If you have a Pinterest account and want to control how your off-Pinterest data is used to tailor your experience, you can visit your [account settings](#) and update your preferences. If you don't have a Pinterest account, or don't want us to customize Pinterest for you when you're signed out, you can opt out [here](#).
- Choose whether your purchases on Pinterest will be used to customize recommendations and ads for you. You can view and manage your purchase history by going to "Order history" in your [account settings](#), and if you hide a purchase from your history, we won't use it to customize Pinterest for you.
- Also, we support the Do Not Track browser setting, and you can [learn more](#) about how it affects our collection and use of off-Pinterest data.
- Close your account at any time. When you close your account, we'll deactivate it and remove your pins and boards from Pinterest. We may retain archived copies of your information as required by law or for legitimate business purposes (including to help address fraud and spam).

In addition to the examples above, we offer other choices that you can learn more about in our [Help Center](#).

You may have choices available to you through the device or software you use to access Pinterest. For example:

- The browser you use may provide you with the ability to control cookies or other types of local data storage.
- Your mobile device may provide you with choices around how and whether location or other data is shared with us.

To learn more about these choices, please see the information provided by the device or software provider.

#### How and when do we share information?

Anyone can see the public boards and Pins you create, and the profile information you give us. We may also make this public information available through what are called "APIs" (basically a technical way to share information quickly). For example, a partner might use a Pinterest API to study what their most popular Pins are or how their Pins are being shared on Pinterest. The other limited instances where we may share your personal information include:

- When we have your consent. This includes sharing information with other services (like Facebook or Twitter) when you've chosen to link to your Pinterest account to those services or publish your activity on Pinterest to them. For example, you can choose to publish your Pins to Facebook or Twitter.
- When you buy something on Pinterest using your credit card, we share your credit card information, contact information, and other information about the transaction with the merchant you're buying from. The merchants treat this information just as if you had made a purchase from their website directly, which means their privacy policies and marketing policies apply to the information we share with them.
- If you buy something on Pinterest using Apple Pay, your credit card number is not shared with the merchant, but contact and transaction information is still shared.
- Online advertisers typically use third party companies to audit the delivery and performance of their ads on websites and apps. We also allow these companies to collect this information on Pinterest. To learn more, please see our [Help Center](#).
- We may employ third party companies or individuals to process personal information on our behalf based on our instructions and in compliance with this Privacy Policy. For example, we share credit card information with the payment companies we use to store your payment information. Or, we may share data with a security consultant to help us get better at identifying spam. In addition, some of the information we request may be collected by third party providers on our behalf. For more information about the providers we use, please see our [Help Center](#).
- If we believe that disclosure is reasonably necessary to comply with a law, regulation or legal request; to protect the safety, rights, or property of the public, any person, or Pinterest; or to detect, prevent, or otherwise address fraud, security or technical issues.



BMW Händlersuche.

# Zielkonflikt 4: Unterschiedliche Interessen von Anwendern und Diensteanbietern vgl. Opt-Out-Cookies beeinträchtigen Privacy und Usability.

All Participating Companies (130) SHOW

Companies Customizing Ads For Your Browser (4)

Existing Opt Outs (0) SHOW

**These 4 participating companies have enabled interest-based ads for this web browser.**

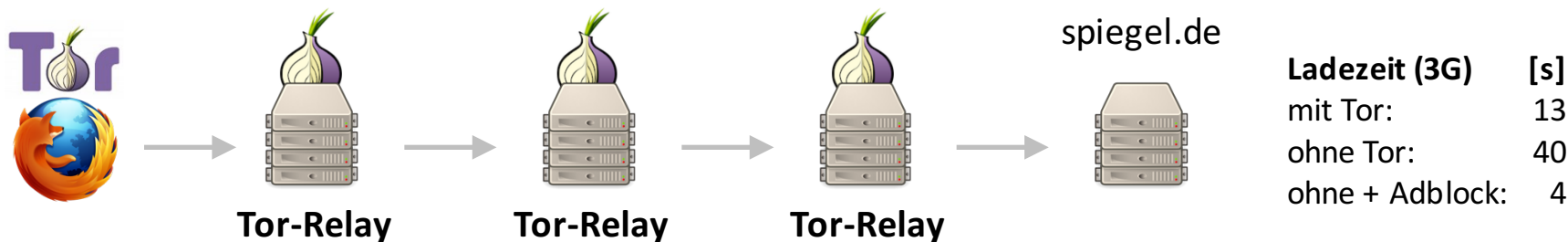
Click the company name to find out more about a participating company. To opt out from interest-based ads by one or more companies, check the box(es) in the "Select" column next to the company name(s), and then hit the "Submit your choices" button. You can also use click the "Select all shown" box to pre-check all the listed companies before you hit the "Submit" button.

[Need help?](#)

COMPANY NAME	SELECT ALL SHOWN <input type="checkbox"/>
Microsoft Advertising	<input type="checkbox"/>
RhythmOne (formerly Burst Media)	<input type="checkbox"/>
Undertone	<input type="checkbox"/>
Yahoo	<input type="checkbox"/>

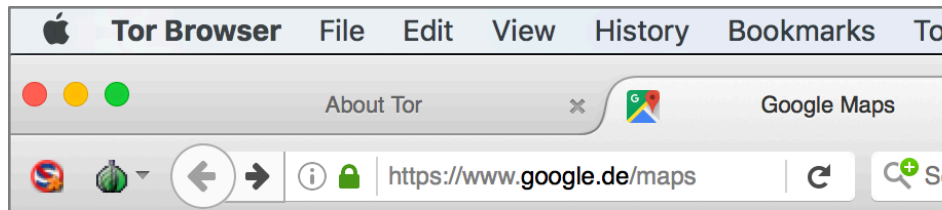
Submitting your choices for the selected companies stores your opt out preference(s) in your browser. [Learn More.](#) Submit your choices

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



**At this security level, the following changes apply (mouseover for details):**

- HTML5 video and audio media become click-to-play via NoScript.
- All JavaScript performance optimizations are disabled. Scripts on some sites may run slower.
- Remote JAR files are blocked.
- Some mechanisms of displaying math equations are disabled.
- Some font rendering features are disabled.
- JavaScript is disabled by default on all sites.
- Some types of images are disabled.
- Some fonts and icons may display incorrectly.



When you have eliminated the JavaScript, whatever remains must be an empty page.

Um Google Maps verwenden zu können, muss JavaScript aktiviert sein.

# Gliederung

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

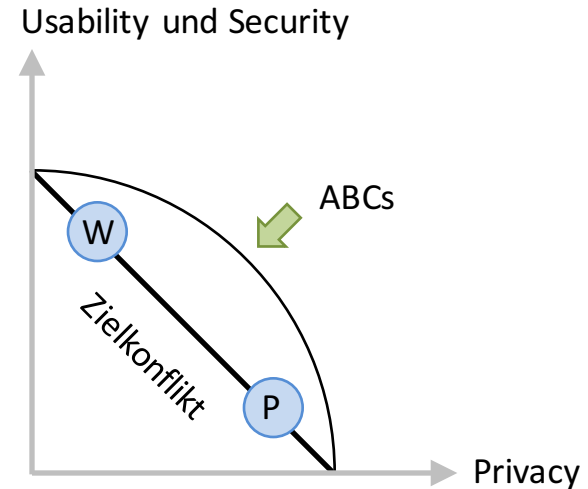
Bei der Evaluation von Lehrveranstaltungen gibt es Zielkonflikte zwischen Anonymität und Authentizität, die sich auf die Usability auswirken.

### Papierbasierte Evaluation (P)

- hoher logistischer Aufwand
- Evaluation nicht an regelmäßige Kursteilnahme geknüpft

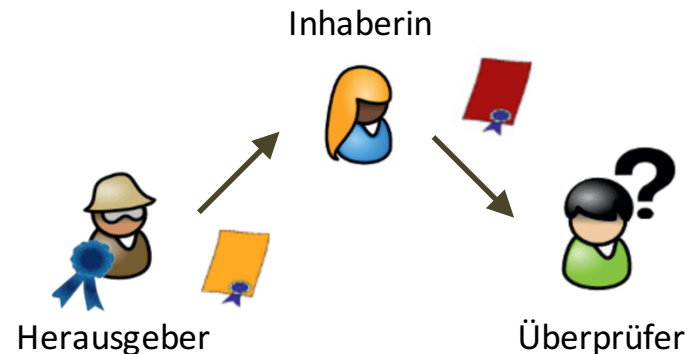
### Webbasierte Evaluation (W)

- Vertrauen in Betreiber nötig



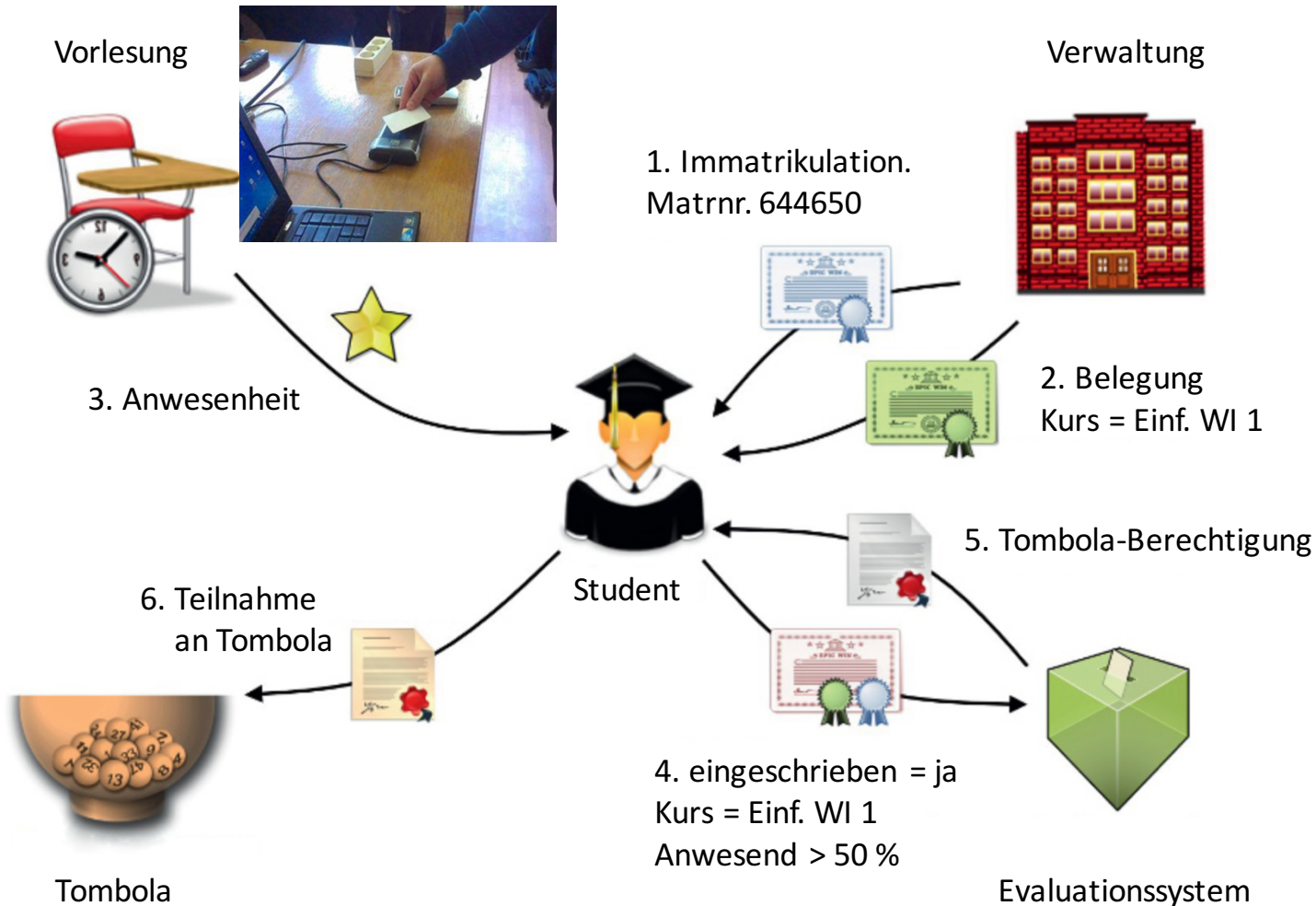
### Attributbasierte Zertifikate (ABCs)

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





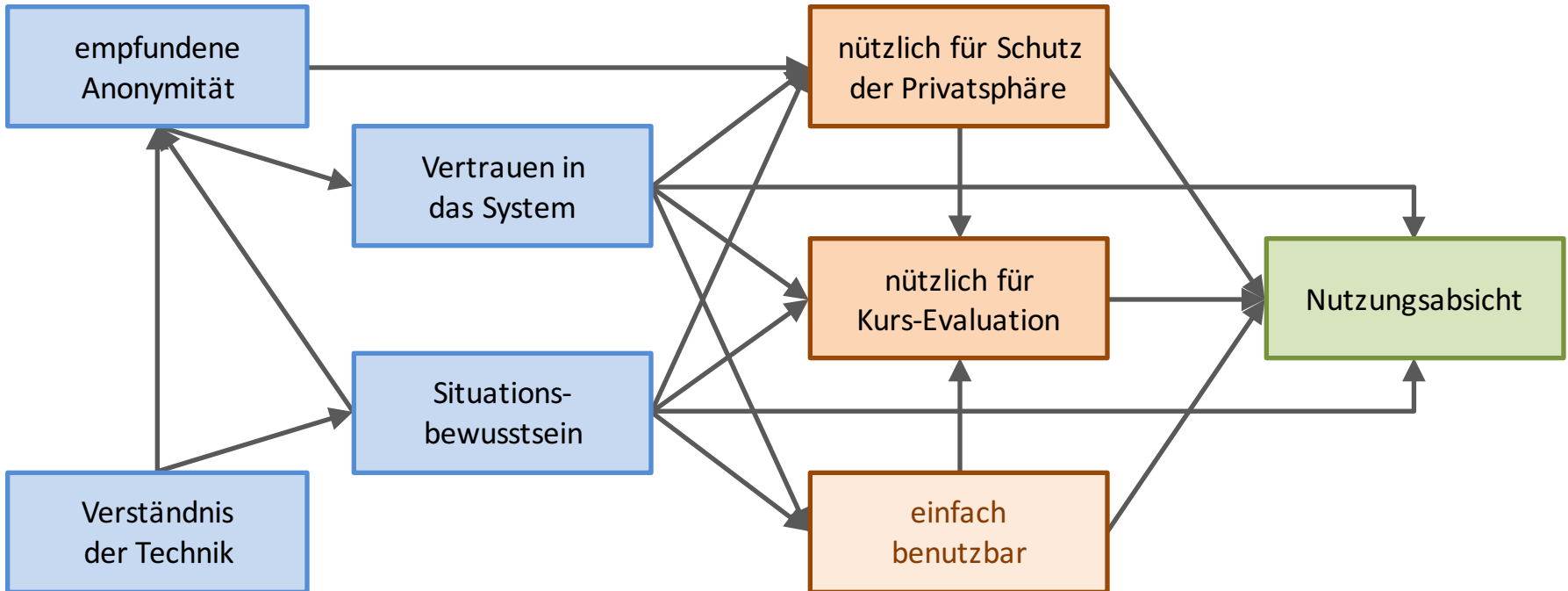
# An der Patras-Universität wurde ein Pilotprojekt durchgeführt, um die Nutzerakzeptanz einer solchen Privacy-by-Design-Lösung zu untersuchen.



# 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.

# Zusammenfassung

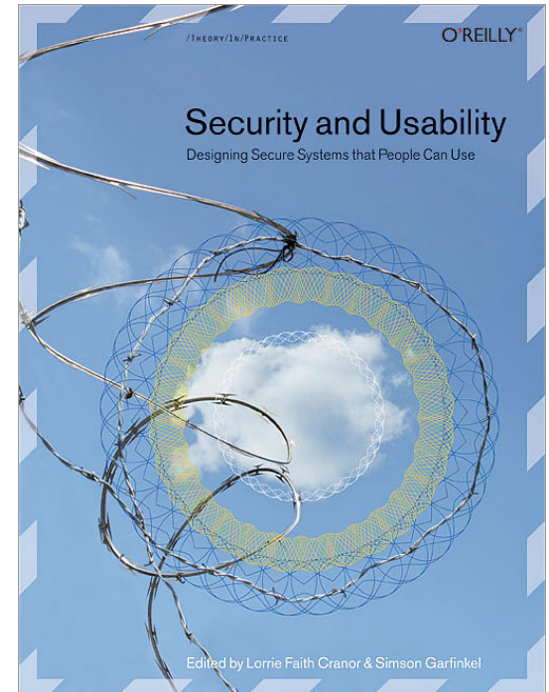
## Zwei Fallstudien

- 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 Selbstschutz-Tools vs. **Entwicklungsaufwand für die Anbieter**

**Privacy by Design:** Benutzbare und sichere Lösungen lassen sich realisieren, wenn Usability und Privacy bereits beim Entwurf berücksichtigt werden.



Cranor & Garfinkel (2014)