AN.ON
NEXT GENERATION

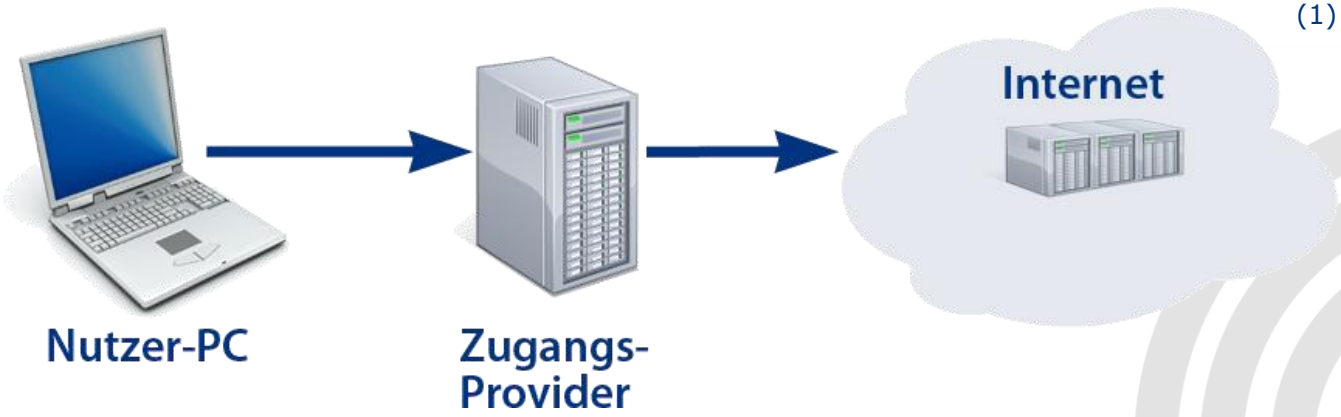
GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Can the ISP be trusted?

Lukas Hartmann, Matthias Marx, Eva Schedel,
Christian Roth, Doğan Kesdoğan

Datenspuren in der digitalen Welt

- Beim Internet-Zugangsanbieter (ISP) bündeln sich die Internetverbindungen eines Nutzers (Verkettung)
  - Gefahr der Profilbildung
- Nutzer haben keine Möglichkeit, die Nutzung oder Weitergabe ihrer Daten durch ISP oder Dritte zu erkennen.

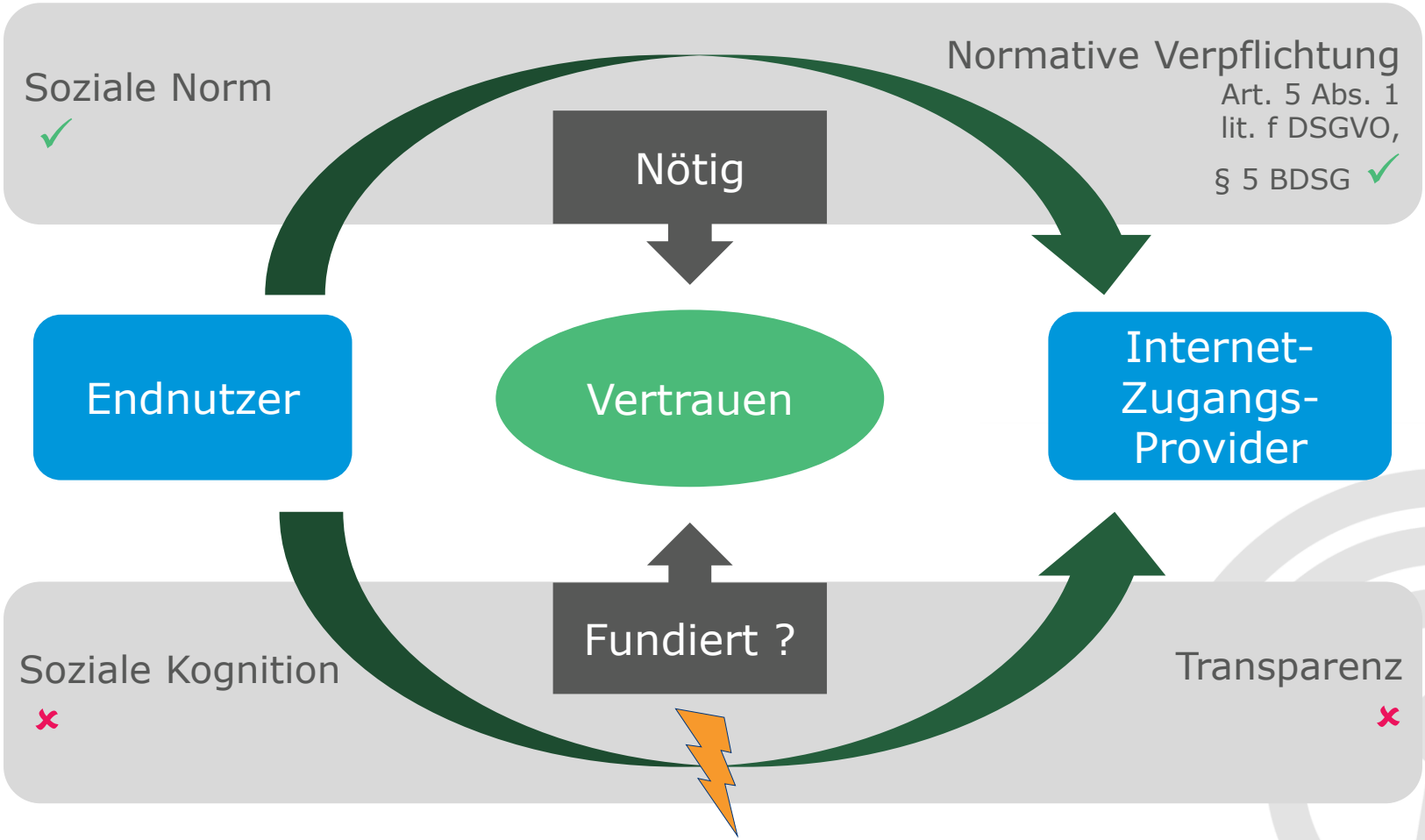


› Wie kann fundiertes Vertrauen geschaffen werden?

Vertrauen

Basis für Vertrauen

Bindung an Vertrauen



Bindung an Recht: Begründung von Vertrauen

§ 88 Telekommunikations-gesetz

Kein Unter-drücken

Kenntnisnahme von Kundendaten nur, soweit erforderlich Abs. 3 S. 1

Zweck-bindung Abs. 3 S. 2

Keine Weitergabe an Dritte Abs. 3 S. 3

§ 202a StGB bei verschlüsselten Daten

§ 206 Abs. 1, 2 Nr. 2 StGB Verletzung Fernmeldegeheimnis

§ 149 Abs. 1 TKG OWi
§ 44 TKG Zivilrechtliche Ansprüche

Internet-zugangs-provider § 3 Nr. 6, 10, 24 TKG

Bindung an Recht: Fragwürdigkeit von Vertrauen

Befugnisse zur <u>Speicherung ohne</u> konkreten <u>Anlass</u>

- **Vorratsdatenspeicherung**
  §§ 113a – g TKG - (noch) geltendes Recht
  Verkehrsdaten (10 Wochen) + Standortdaten (4 Wochen)

- **Erkennen von Störungen** etc.
  § 100 TKG (IT-Sicherheitsgesetz)
  Bestandsdaten + Verkehrsdaten + „Steuerdaten"
  („höchstens" 7 Tage – „kleine Vorratsdatenspeicherung")

<u>Voraussetzungsarmer, intransparenter Zugriff</u>

- **Automatisierte Abfragemöglichkeit**
  § 112 Abs. 1 TKG
  Bestandsdaten („Kundendatei") - Stellen Personenbezug her!

Bindung an Recht: Fragwürdigkeit von Vertrauen

Fazit

- **Sanktionsmöglichkeiten motivieren** ISPs eher **zu übermäßiger Speicherung** als Datensparsamkeit, vgl. § 126 Abs. 4 TKG
- ISP selbst hat **keine volle Kontrolle**
  - Automatisierter Zugriff auf Bestandsdaten
  - Mit Richtervorbehalt auch auf weitere Daten

› Den Schutzmechanismen für Vertraulichkeit stehen **erhebliche Risiken** gegenüber.

Problemfaktoren für Privacy Behavior beim Nutzer (I)

- **Informationsdefizit**
  - **Vertrauenswürdigkeit und Verlässlichkeit** des ISP
  - **welche Daten** des Nutzers der ISP kontrolliert
  - **mögliche Konsequenzen** eines Datenmissbrauchs

  Problemstellung in der Vorstellung des Nutzers evtl. gar nicht abgebildet.

- **Schwierigkeit, nach den eigenen Präferenzen zu entscheiden**
  - **Begrenzte kognitive Ressourcen bei hoher Komplexität** („Security Fatigue“)
  - **Problem der begrenzten Rationalität**
  - Datenschutz immer **Kompromissen** unterworfen (Nutzen aus Datenpreisgabe, „Privacy attitudes“)
  - **Entgegengerichtete Einflüsse** (soziale Normen, Motivation, Emotionen)

Problemfaktoren für Privacy Behavior beim Nutzer (II)

- **Kontextabhängigkeit**
  - Fehlender **Bezugsrahmen** in der digitalen Welt, Abstraktheit
  - **Gewöhnung** an gleichbleibende Beeinträchtigungen der Privatsphäre

- **Beeinflussbarkeit**
  - Bedingt durch **Informationsmangel und Kontextabhängigkeit**
  - Beispiel **Default settings: häufig als Empfehlung aufgefasst**
  - Beispiel **Features, welche durch ihr bloßes Vorhandensein ungerechtfertigtes Vertrauen auslösen** (Privacy Policy, Privatsphäre-Einstellmöglichkeiten)

I. Transparenz

*Aus der Privacy Behavior – Forschung lassen sich **Anforderungen** für technische Lösungen ableiten. Diese Anforderungen können den **Datenschutz-Gewährleistungszielen** des **Standard-Datenschutzmodells** zugeordnet werden:* Transparenz + Intervenierbarkeit. Zum dritten Datenschutz-Gewährleistungsziel, Nichtverkettung, siehe Folie 1.

- **Information**
  Bedeutungsgehalt vermitteln.
- **Verifikation** (Nachweis)
  Abbilden einer tatsächlichen Gegebenheit
  mit angemessener Sicherheit / Wahrscheinlichkeit.
- **Verständlichkeit**
  Bedeutung für Durchschnittsnutzer ohne weiteres zu erfassen. Reduktion von Komplexität.

II. Intervenierbarkeit

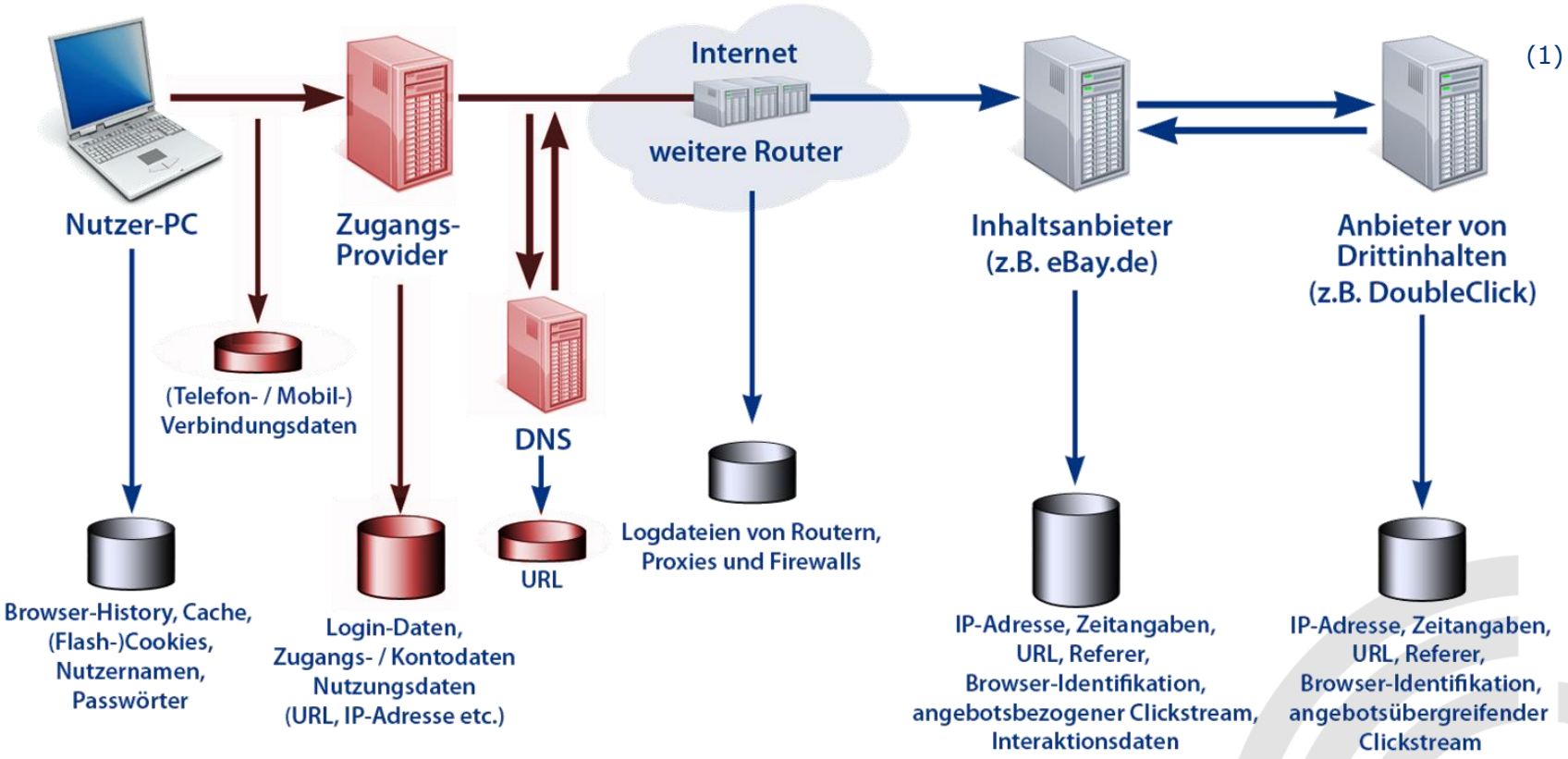
- **Relevanz**
  Empfundene Bedeutung für die eigene Person.
- **Auffälligkeit** (Salienz)
  Aufmerksamkeit des Nutzers wird wirksam auf bedeutsame Aspekte gelenkt.
- **Orientierung**
  Bezugsrahmen als Orientierung. Empfehlungen als Anker. Implikationen einer Privatsphäre-Verletzung erkennbar. Reduktion kognitiver Beanspruchung.
- **Handlungsmöglichkeit** für den Nutzer
  Möglichkeit bereitzustellen, reale Kontrolle auszuüben.

Zwischenfazit

- Verwirklichung von Datenschutz und Privatsphäre allein durch das **Recht** nicht möglich.
- Handeln im wohlverstandenen eigenen Interesse erfordert echte Akkommodation an die digitale Welt.
- **Psychologische** Forschung zum Privacy Behavior liefert Hinweise, wie **fundiertes Vertrauen** erreicht werden kann.

› Kann die **Technik Lösungen** bereitstellen?

Der Weg der persönlichen Daten



› Nutzer wissen oft nicht, welche Parteien welche Informationen über ihn kennen

Transparency Enhancing Technologies

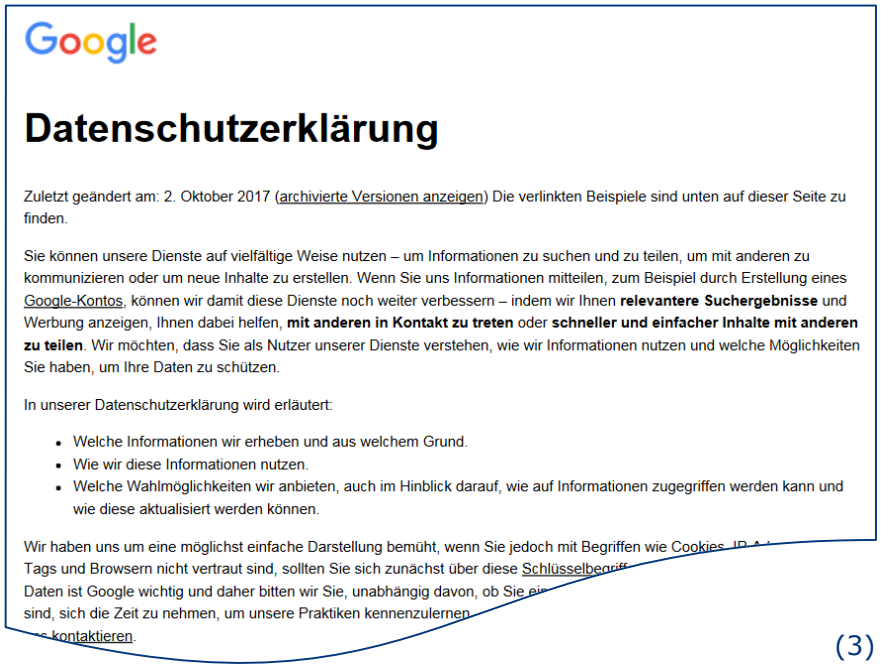
- *"Legal and technological instruments that provide […] access to data processing, implying a **transfer of knowledge** from data controller to data subject […]"* (2)

- Anforderungen an TETs leiten sich von **Nutzersicht** ab

- Verschiedene Strategien möglich

Strategie Policy

- Auflistung, welche Daten gespeichert und verarbeitet werden.
  - Beispiel: Google Datenschutzerklärung



Google

Datenschutzerklärung

Zuletzt geändert am: 2. Oktober 2017 (archivierte Versionen anzeigen) Die verlinkten Beispiele sind unten auf dieser Seite zu finden.

Sie können unsere Dienste auf vielfältige Weise nutzen – um Informationen zu suchen und zu teilen, um mit anderen zu kommunizieren oder um neue Inhalte zu erstellen. Wenn Sie uns Informationen mitteilen, zum Beispiel durch Erstellung eines Google-Kontos, können wir damit diese Dienste noch weiter verbessern – indem wir Ihnen **relevantere Suchergebnisse** und Werbung anzeigen, Ihnen dabei helfen, **mit anderen in Kontakt zu treten** oder **schneller und einfacher Inhalte mit anderen zu teilen**. Wir möchten, dass Sie als Nutzer unserer Dienste verstehen, wie wir Informationen nutzen und welche Möglichkeiten Sie haben, um Ihre Daten zu schützen.

In unserer Datenschutzerklärung wird erläutert:

- Welche Informationen wir erheben und aus welchem Grund.
- Wie wir diese Informationen nutzen.
- Welche Wahlmöglichkeiten wir anbieten, auch im Hinblick darauf, wie auf Informationen zugegriffen werden kann und wie diese aktualisiert werden können.

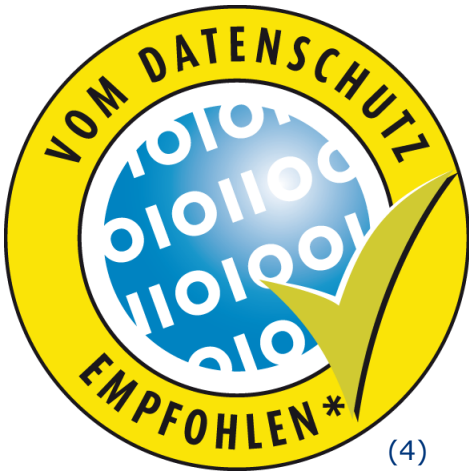
Wir haben uns um eine möglichst einfache Darstellung bemüht, wenn Sie jedoch mit Begriffen wie Cookies, IP-A... Tags und Browsern nicht vertraut sind, sollten Sie sich zunächst über diese Schlüsselbegriff... Daten ist Google wichtig und daher bitten wir Sie, unabhängig davon, ob Sie ei... sind, sich die Zeit zu nehmen, um unsere Praktiken kennenzulernen... ...kontaktieren.

(3)

Eigenschaften	
Information	✓
Verifikation	✗
Verständlichkeit	✗
Relevanz	✗
Auffälligkeit	✗
Orientierung	✗
Handlungs-möglichkeiten	✗

Strategie Siegel

- Nutzer vertraut auf Siegel einer dritten Instanz, die Privatsphäre bewertet
  - Beispiel: Datenschutzsiegel ULD, TÜV Süd



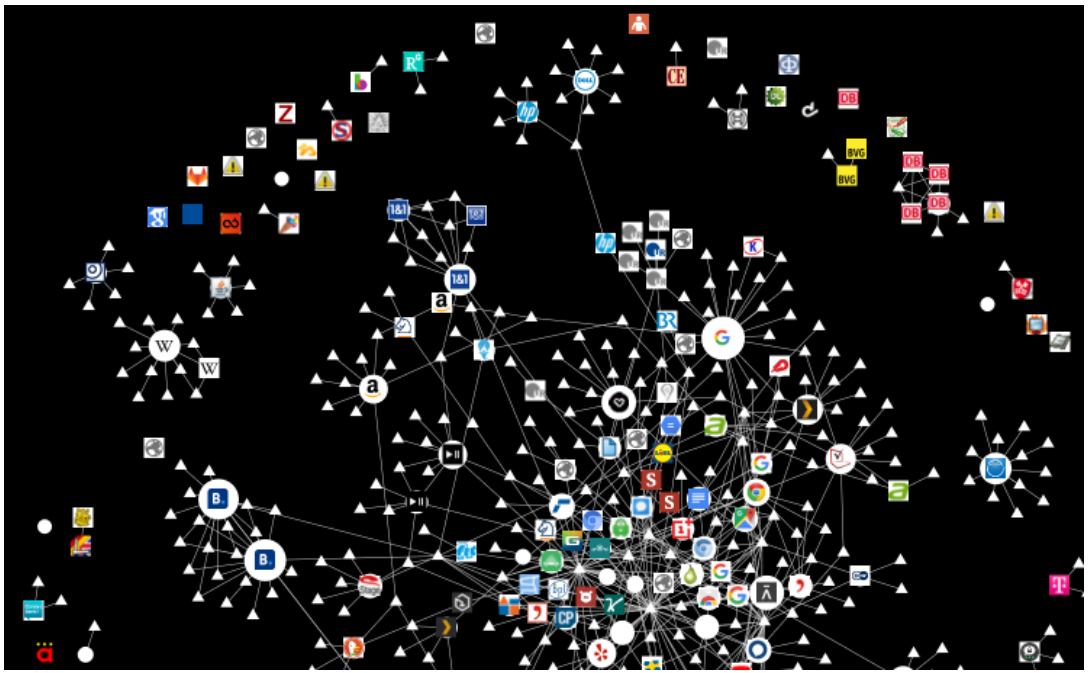
(4)

(5)

Eigenschaften	
Information	✓
Verifikation	✗
Verständlichkeit	✓
Relevanz	✗
Auffälligkeit	✗
Orientierung	✓
Handlungs-möglichkeiten	✗

Strategie Software

- Nutzerdaten werden aufbereitet dargestellt und somit Relevanz verdeutlicht
  - Beispiel: Lightbeam für Mozilla Firefox

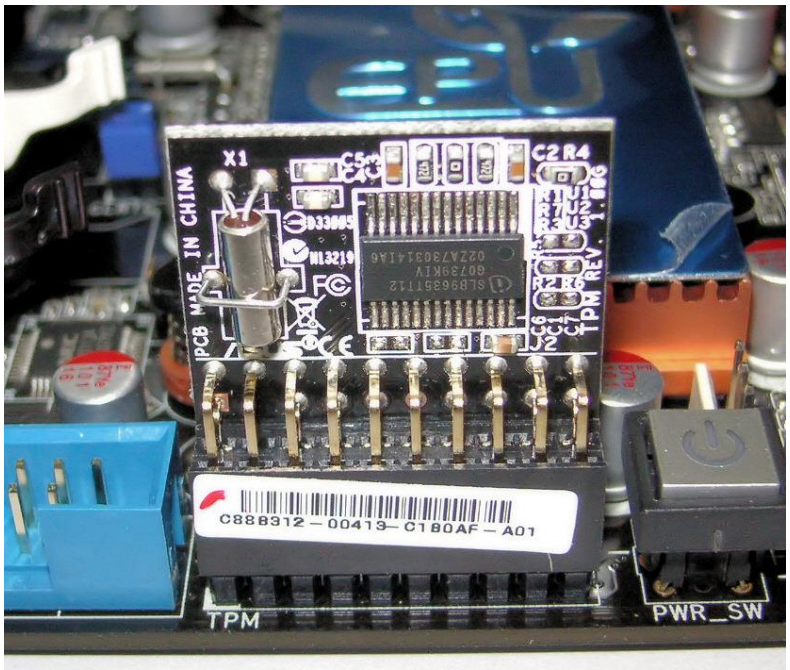


(6)

Eigenschaften	
Information	✓
Verifikation	✗
Verständlichkeit	✓
Relevanz	✓
Auffälligkeit	✓
Orientierung	✗
Handlungs-möglichkeiten	✗

Strategie Hardware

- Zusätzliche Hardware überprüft Einhaltung und informiert ggf. Nutzer.
  - Beispiel: Trusted Computing



(7)

Eigenschaften	
Information	✗
Verifikation	✓
Verständlichkeit	✗
Relevanz	✗
Auffälligkeit	✗
Orientierung	✗
Handlungs-möglichkeiten	✗

Limitationen von TETs

- TETs benötigen selbst Zugriff auf Daten
- Datenaggregation schwierig abbildbar
- TETs können falsches Vertrauen schaffen
- Notwendigkeit einer vertrauenswürdige Dritten Partei, die Integrität der TETs überwacht
- Effektivität wird durch Nutzerverständnis begrenzt

Fazit

- Nutzer benötigen erweiterte Techniken zur Kontrolle ihrer eigenen Daten
- TETS sind hierfür ein erster Schritt
  - Motivation, Veranschaulichung, Edukation
  - Sind limitiert in dem, was sie leisten können
- Vertrauen in den ISP kann technisch nur unzureichend abgebildet werden
  - Anonymisierungs-Lösungen beim ISP schützen nur vor schwachen Angreifern
  - Für stärkeren Schutz sind zusätzliche Techniken nötig

Ausblick

- Rechtliche Vorgaben können unterstützen
  - Implementierung von TETs und somit
  - Grundlegende Schutzmaßnahmen beim ISP
- Wirtschaftliche Aspekte müssen für massen-taugliche Lösung ebenfalls betrachtet werden
  - Für institutionelles Vertrauen ist **Reputation** von zentraler Bedeutung

› Fundiertes Vertrauen kann nur **interdisziplinär** geschaffen werden

Kontakt

Lukas Hartmann · lukas.hartmann@ur.de
Lehrstuhl für Wirtschaftsinformatik IV
Universität Regensburg

Matthias Marx · marx@informatik.uni-hamburg.de
FB Informatik - Sicherheit in Verteilten Systemen
Universität Hamburg

Eva Schedel · uld66@datenschutzzentrum.de
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein (ULD)

Quellen

(1) Abgeändert; nach Marit Hansen: "Spuren im Netz - der Schutz der Privatsphäre". In: Dieter Korczak (Hrsg.): Spurensuche. Kulturwissenschaftliche Interpretationen und gesellschaftliche Rezeption. Kröning: Asanger (2010), S. 105-128

(2) Hildebrandt, Mireille (2009). Profiling and AmI. In The Future of Identity in the Information Society. (Springer Berlin Heidelberg), S. 273–310.

(3) Google Datenschutzerklärung, https://static.googleusercontent.com/media/www.google.com/de//intl/de/policies/privacy/google_privacy_policy_de.pdf (abgerufen am 23.10.2017)

(4) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/guetesiegel/ (abgerufen am 23.10.2017)

(5) TÜV Süd, www.tuev-sued.de/ms/iso-27001 (abgerufen am 23.10.2017)

(6) Firefox Lightbeam Add-On, https://addons.mozilla.org/en-US/firefox/addon/lightbeam/ (abgerufen am 23.10.2017)

(7) FxJ (Own work) [Public domain], via Wikimedia Commons

AN.ON
NEXT GENERATION

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Can the ISP be trusted?

Lukas Hartmann, Matthias Marx, Eva Schedel,
Christian Roth, Doğan Kesdoğan