Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Der elektronische Datenbrief
als aktive
informationelle Selbstbestimmung

Prof. Dr. (TU NN)
Norbert Pohlmann
Maik Heidisch

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Inhalt

- Motivation
- Datenbrief
- Elektronischer Datenbrief / Online Privacy Service
- Bewertung der aktuelle Situation
- Fazit und Ausblick

Inhalt

- **Motivation**
- Datenbrief
- Elektronischer Datenbrief / Online Privacy Service
- Bewertung der aktuelle Situation
- Fazit und Ausblick

Motivation
→ Vertrauen in neue Technogien

Vertrauen [Wikipedia]

- Unter Vertrauen wird die Annahme verstanden, dass Entwicklungen einen positiven oder erwarteten Verlauf nehmen.

- **Ein wichtiges Merkmal ist dabei das Vorhandensein einer Handlungsalternative.**

Informationelle Selbstbestimmung

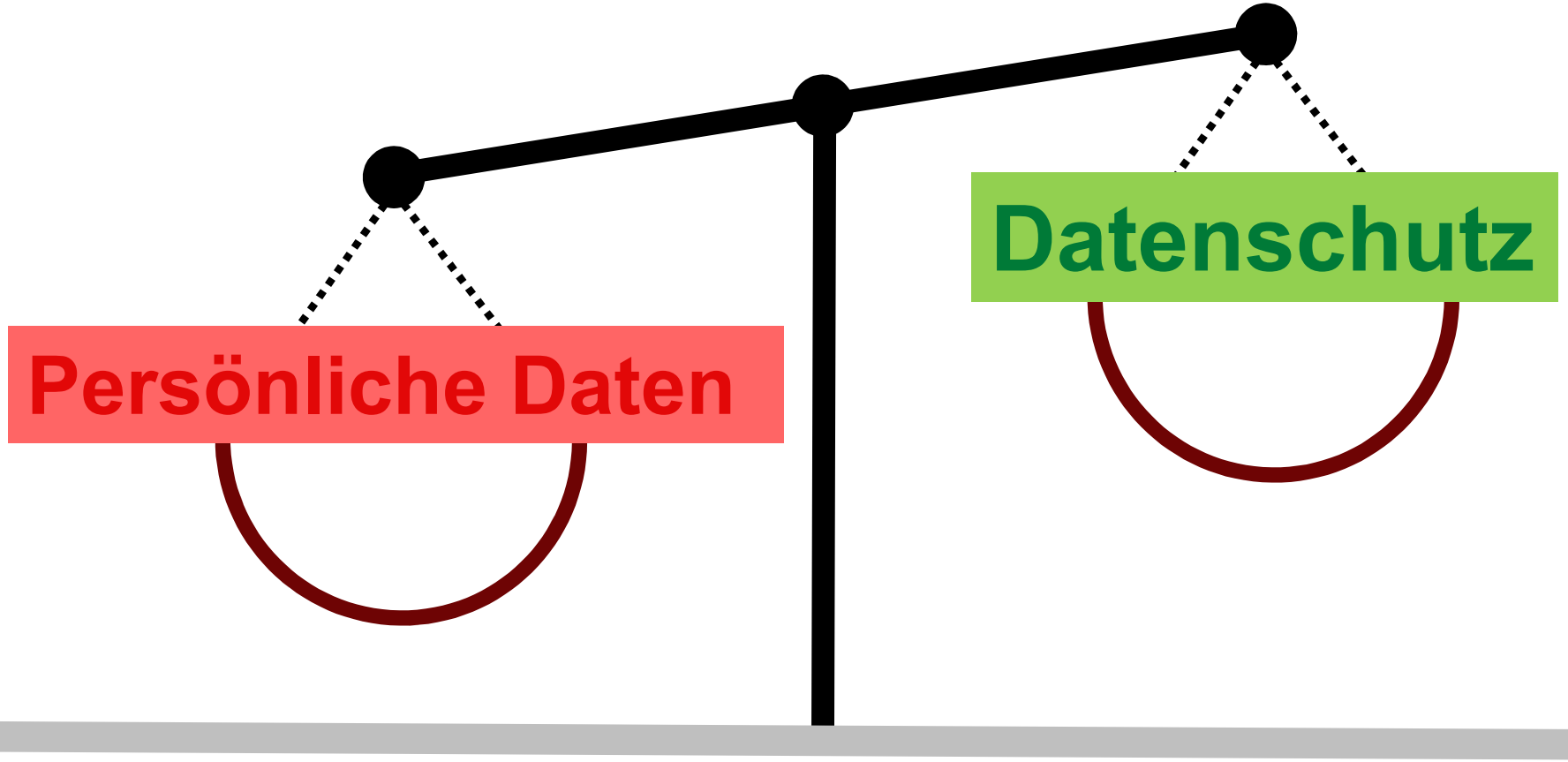
- **Recht auf informationelle Selbstbestimmung in Deutschland**
  - Befugnis des Einzelnen selbst über die Preisgabe und Verwendung der persönlichen Daten zu bestimmen

- **Elektronische Datenbrief**
  - Idee, die aktive informationelle Selbstbestimmung im Internet pragmatisch möglich zu machen

Die Datenschutzsituation heute
→ Eine kritische Bewertung (1/5)

Persönliche Daten sind ein Rohstoff

des Internetzeitalters



Die Datenschutzsituation heute
→ Eine kritische Bewertung (2/5)

Geschäftsmodell: „Bezahlen mit persönlichen Daten“

- **Soziale Netzwerke** (Facebook, …), **E-Mail-Dienste** (Google , …), … **verdienen ihr Geld** vor allem **mit Werbung !**
- Je besser die Internet-Dienstanbieter die Internet-Nutzer kennen, desto mehr Geld können sie verdienen.
- Die Nutzer zahlen **kein Geld** für den Internet-Dienst!
- **Die Nutzer stimmen über die AGBs zu, dass der Internet-Betreiber alle persönlichen Daten für eine Profilbildung nutzen darf und damit Werbegeld einnehmen kann.**
- Die Internet-Dienstanbieter verdienen mit **individualisierter Werbung sehr viel Geld** (**Google 2009 ca. 24 Milliarden US-Dollar!**).
- **aber**
  individualisierte Werbung ist auch ein Feature, das viele Internet-Nutzer *sehr gut* finden!

Die Datenschutzsituation heute
→ Eine kritische Bewertung (3/5)

Beispiel: Google (1/2)

Bei der Nutzung vieler Google-Dienste weiß Google,

- wer man ist und wo man wohnt (Buzz, Checkout, Gmail, Profiles etc.)
- welche sozialen Kontakte man pflegt (Buzz, Gmail, Orkut, Talk, Voice etc.)
- wo man sich gerade aufhält (Ortung per GSM-Zelle, GPS oder WLAN bei Google's mobilen Diensten wie Latitude, Navigation oder Near me now …)
- Wohin man will (Earth, Maps, Navigation etc.)
- welche Termine man hat (Kalender, Sync etc.)
- welche Interessen man hat (diverse Suchdienste sowie weitere Dienste und Produkte wie Analytics, Blogger.com, Buzz, Chrome, Gmail, Groups, iGoogle, Knol, YouTube u.v.m.)
- wie die Bankverbindung lautet (Checkout)

Die Datenschutzsituation heute
→ Eine kritische Bewertung (4/5)

Beispiel: Google (2/2)

Bei der Nutzung vieler Google-Dienste weiß Google,

- wer die Partner bei Finanzgeschäften sind, was man kauft, wie viel man dafür ausgibt und wann Geschäfte abgewickelt werden (Checkout)
- welche und wie viele Aktien(-fonds) man besitzt und welche Transaktionen man diesbezüglich abwickelt (Finance)
- wie die eigene DNA aussieht und was für Krankheiten man hat oder hatte, einschließlich entsprechender Therapien (Health)
- wie man aussieht (Buzz, Gmail, Picasa, Profiles etc.)
- welche Daten man allgemein am eigenen Rechner bearbeitet (Chrome OS und weitere Cloud Computing-Angebote)
- usw.

Studie: Google – die zwei Seiten des mächtigen Internet-Konzerns
www.internet-sicherheit.de/fileadmin/docs/publikationen/2011/Google-StudieV2.0.pdf

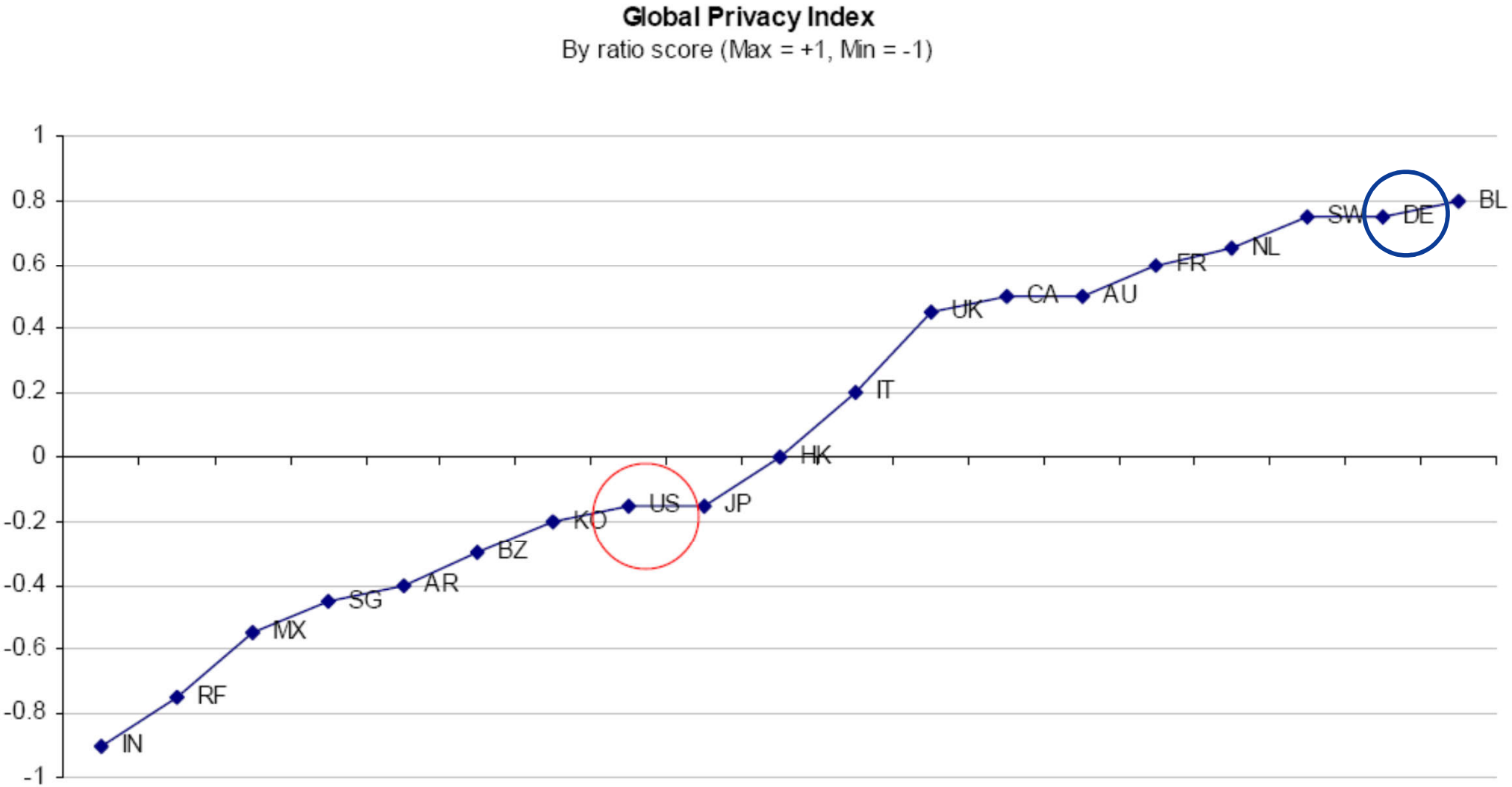
Die Datenschutzsituation heute
→ Eine kritische Bewertung (5/5)

Probleme: Protokoll-Daten überall

```
91.51.162.241 - - [12/Sep/2009:11:41:32 +0200] „GET
/fileadmin/template/images/partner/logo-ifis-lehre.gif“
HTTP/1.1“ 200 2069 „http://www.internet-
sicherheit.de/forschung/aktuelle-
forschungsprojekte/internet-fruehwarnsysteme/“ „Mozilla/5.0
(X11;U;Linux i686; de-DE; rv:1.9.0.13) Gecko/2009082610
Gentoo Firefox/3.0.13“
```

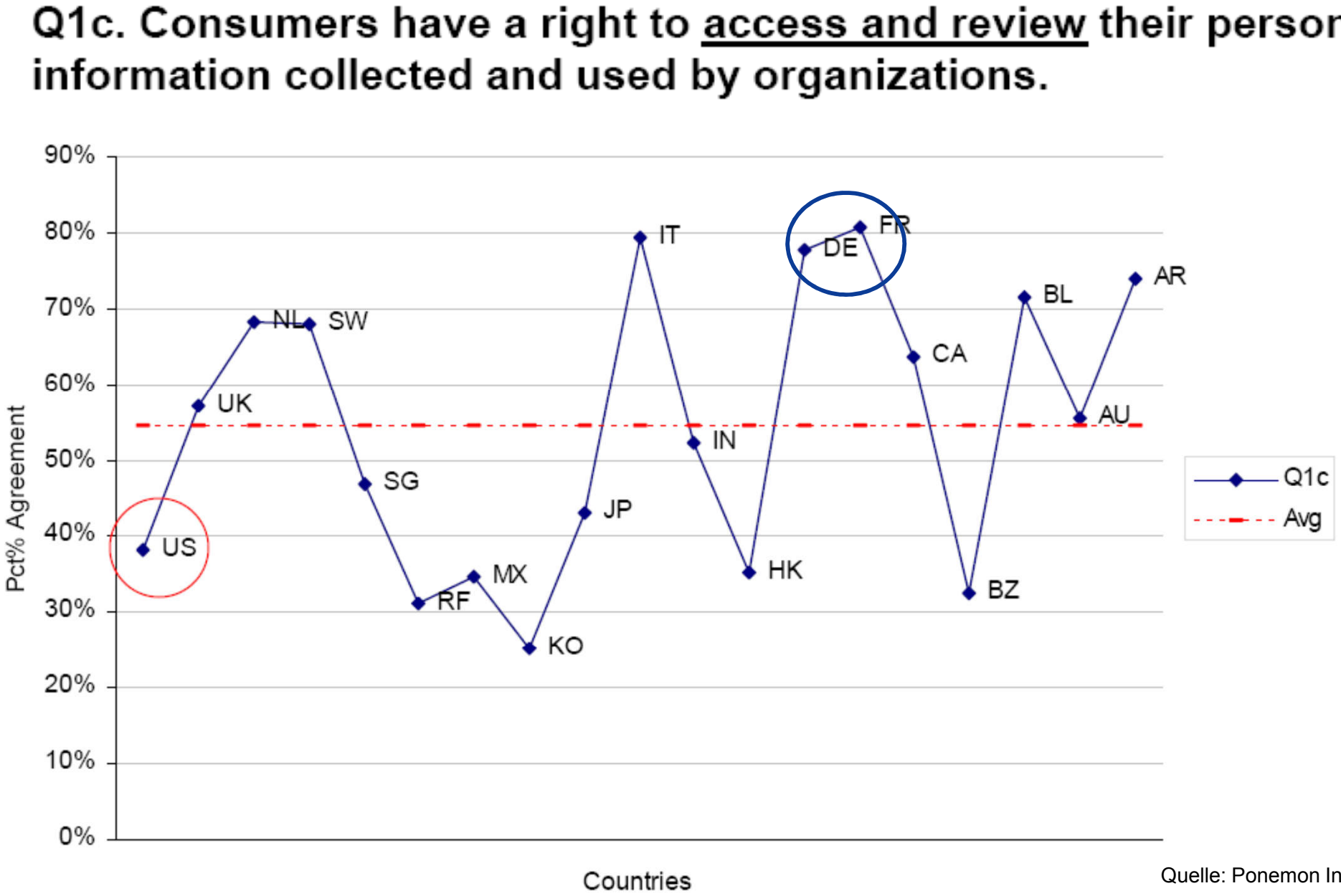
- **Spuren der Nutzer im Internet**
  - Browser (**Cookies**, **Browser-History**, spezielle Toolbars, …)
  - Webserver (Log, Google-Analytics, Proxy-Server, …)
  - Mail-, SIP-, DNS-Server, …
  - Router, IDS, Firewalls, … (Infrastrukturkomponenten)
  - **SmartPhones (IDs, Positionsbestimmung: GPS, GSM und WLAN)**
  - **Gefällt-Mir-Button**
  - …

Privacy Paranoia
→ Exkurs: 1/2



Quelle: Ponemon Institute

Privacy Paranoia
→ Exkurs: 2/2



Quelle: Ponemon Institute

Inhalt

- Motivation
- **Datenbrief**
- Elektronischer Datenbrief / Online Privacy Service
- Bewertung der aktuelle Situation
- Fazit und Ausblick

Datenbrief
→ Überblick

- **Der Datenbrief ist eine Forderung des Chaos Computer Clubs!**

- **Inhalt des Datenbriefs**
  - Persönliche Daten und deren Ursprung
  - Angereicherte Daten: Profile, Scoring-Werte, …
  - Zweck und Rechtsgrundlage für die Speicherung

- **Randbedingungen des Datenbriefs**
  - Verpflichtung für Firmen, Behörden, Institutionen
  - Kostenlos und regelmäßig
  - Übermittlung postalisch oder elektronisch

- **Aktuell nach BDSG bereits Recht auf Auskunft**
  - Gegebenenfalls ist nicht bekannt, welche Stellen Daten speichern
  - Oft aufwendige Identifikation mittels Personalausweis oder PostIdent nötig

Datenbrief
→ Vorteile

- **Überblick und Kontrolle der eigenen persönlichen Daten bei den genutzten Internet-Diensten**
- **Regelmäßige Konfrontation mit dem Umfang der gespeicherten Daten**
  - Sensibilisierung der Nutzer (Bürger) für den Umgang mit persönlichen Daten
- **Richtigkeit der persönlichen Daten kann überprüft werden**
  - Korrektur- oder Widerspruchsmöglichkeit ist verpflichtend
- **Überprüfung der Legalität der Speicherung möglich**
  - Rechtsgrundlage für die Speicherung der persönlichen Daten muss enthalten sein
- **Mehraufwand der Dienstanbieter bewirkt eine kritische Prüfung der Datenspeicherung**
  - Datenanhäufungen werden unattraktiver

Datenbrief
→ Kritik

- **Fehladressierungen von hochsensiblen und persönlichen Daten durch veraltete Datensätze an Eltern, Ex-Lebenspartner, usw. möglich**
- Zentralisierung der Daten und Schaffung eines potentiellen Angriffsziels
- **Versendung durch Dienstleister zur Reduzierung des Aufwands möglich**
  - Falsch zugestellte Briefe bieten ein Missbrauchspotential
- **Zusammenführung und Aufbereitung der persönlichen Daten nötig**
  - Höherer Wert der Daten fördert den Datenhandel
- **Hohe Kosten müssen kompensiert werden**
  - Z.B. durch Werbung und Preiserhöhungen
- **Datenbrief bietet ein hohes Sicherheitsrisiko**
  - Unverschlüsselter Versand
  - Hochsensible Daten landen ggf. unvernichtet im Hausmüll

Datenbrief
→ Meinung der Politik

- Datenbrief wurde **2010 auch in der Politik diskutiert**
- Damaliger **Bundesinnenminister de Maizière** und **Bundesjustitzministerin Leutheusser-Schnarrenberger** zeigten sich **Anfang 2010 aufgeschlossen**
- Auch der **Bundesdatenschutzbeauftragte Schaar** bezeichnete den Datenbrief **Anfang 2010** als **sinnvoll**
- Im **Mai 2010 relativierten Leutheusser-Schnarrenberger** und **Schaar** jedoch ihre **Meinung**, da es unter **praktischen Gesichtspunkten Probleme** gibt
- **„Anliegen absolut unterstützenswert, aber noch nicht ganz zu Ende gedacht“**

Inhalt

- Motivation
- Datenbrief
- **Elektronischer Datenbrief / Online Privacy Service**
- Bewertung der aktuelle Situation
- Fazit und Ausblick

Online Privacy Service (OPS)
→ Überblick: Elektronischer Datenbrief

- **Online Privacy Service bietet prinzipiell die selben Möglichkeiten wie der Datenbrief**

- **Standardisierter Online Privacy Service zur Bearbeitung gespeicherter persönlicher Daten**
  - Verpflichtung von Firmen, Behörden und Institutionen mit Onlinedienst
  - Kostenlose Bearbeitung und Abruf jederzeit möglich
  - In bestehenden Dienst integrierbar (Verwendung des bestehenden Logins)

- **Regelmäßige Benachrichtigung über Speicherung**
  - Dient als Erinnerung, gespeicherte persönlicher Daten wiederholt zu überprüfen

- **Information über Ersterfassung bei Datenspeicherung ohne Konto**
  - Zugangsdaten müssen nach Identifikation einzurichten sein
  - Liegt keine Kommunikationsmöglichkeit vor, muss die Speicherung unzulässig sein!

Online Privacy Service (OPS)
→ Widerspruchsmöglichkeit

- **Elektronische Korrektur sowie Widerspruch ist möglich**

- **Korrektur bedeutet auch Optimierung der Werbung**
  - WIN-WIN Situation zwischen Dienste-Anbieter und Nutzer!

- **Widerspruch bedeutet, dass alle persönlichen Daten komplett gelöscht werden können**
  - Die **Grundlage** für eine personalisierte Werbung ist abschaltbar!
  - Impliziert ggf. Umwandlung in kostenpflichtigen Dienst
    - Reicht normale Werbung oder
    - mit Geld zahlen statt mit persönlichen Daten

Online Privacy Service (OPS)
→ Standardisierung

- **Online Privacy Service muss standardisiert sein**
  - Gewährleistung eines einheitlichen, einfachen und sicheren Zugriffs
  - Ermöglicht schnelle Akzeptanz und Einarbeitung durch die Bürger (Nutzer)
    - Gleiche Bedienung, gleiches Aussehen, gleiche Bedeutung, …

- **Sichere Umsetzung der Integration in die jeweiligen Internet-Dienste**
  - Verwendung von SSL/TLS
  - Schutz gegen Angriffe auf die gespeicherten Daten

- **Zusätzliche nutzbare Schnittstelle, die den Abruf der persönlichen Daten über eine spezielle OPS-Anwendung ermöglicht**
  - Persönliche Daten verschiedener Stellen können damit von einer OPS-Anwendung zusammengeführt werden
  - Ermöglicht eine globale Sichtweise aller gesammelten Daten einer Person im Internet
  - Ist sehr hilfreich, um Entscheidungen für die einzelnen Internet-Dienste zu treffen

Online Privacy Service (OPS)
→ Vergleich

- Die eigenen persönlichen Daten können **zur jeder Zeit** überblickt und kontrolliert werden

- **Kein Missbrauchspotential durch Fehladressierung**
  - Nutzung gleicher Zugangsdaten
  - Registration benötigt Identifikation

- **Keine Sicherheitsrisiken durch unverschlüsselten Versand der Briefe**
  - Standardisierter Online Privacy Service

- **Kosten**
  - Im Prinzip nur einmalige Kosten für die Bereitstellung des Dienstes

Inhalt

- Motivation
- Datenbrief
- Elektronischer Datenbrief / Online Privacy Service
- **Bewertung der aktuelle Situation**
- Fazit und Ausblick

Aktuelle Situation
→ Facebook (1/2)

- **Speicherung von über 100 verschiedenen Datensätzen**

- **Datenanforderung von Max Schrems im Juni 2011**
  - Erhalt von 1.222 Seiten mit 57 Datensätzen
  - 22 Datensätze mit Profilinformationen, 35 Datensätze mit generierten Daten

- **Hoher Zuwachs an Anfragen durch die Initiative von Schrems**
  - Datendownload seit November 2011 möglich
  - Download enthält lediglich die Profilinformationen
  - Stellt Irritation des Benutzers dar
  - Keine volle Dateneinsicht, da generierte Daten nicht enthalten sind

Aktuelle Situation
→ Facebook (2/2)

- **Ansicht der herunterladbaren Profilinformationen auf Facebook**

Profil

Pinnwand

Fotos

Freunde

Nachrichten

Max Mustermann

Facebook-Profil:	http://www.facebook.com/profile.php?id=100000123456789
Derzeitiger Wohnort:	Musterstadt, Germany
E-Mail:	max.mustermann@example.com
Geburtstag:	01/01/1970
Geschlecht:	Männlich
Beziehungsstatus:	Single
Heimatstadt:	Musterstadt
Ausbildung:	Allgemeine Hochschulreife (Abitur) - 1989

Aktuelle Situation
→ SCHUFA (1/3)

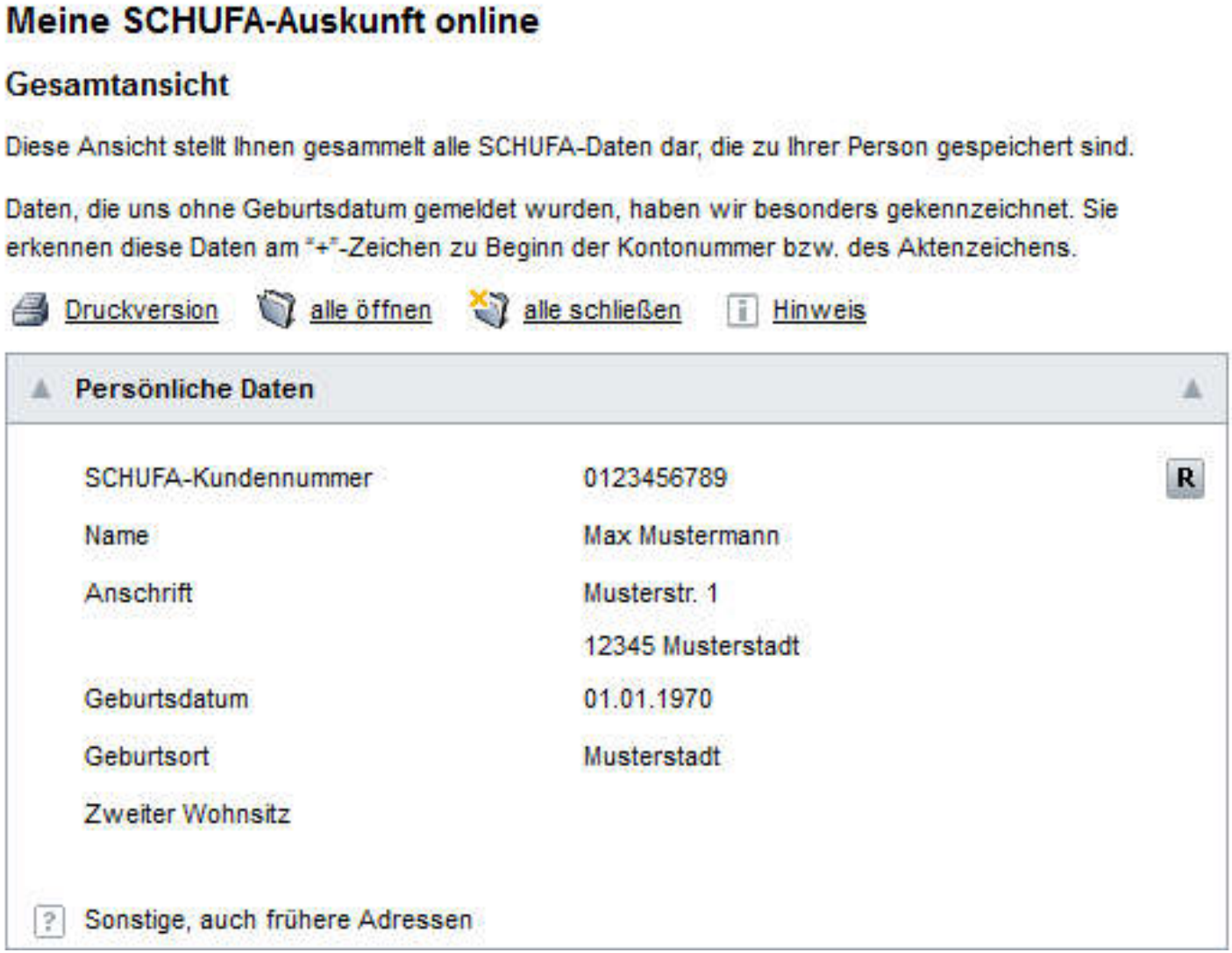
- **Nach kostenpflichtiger Registrierung kann jederzeit auf die gespeicherten Daten zugegriffen werden**
  - Über „Rückfragen“ können Korrekturen und ein Widerruf beantragt werden
  - Automatische Benachrichtigungen über Änderungen sind kostenpflichtig

- **Es werden nicht alle Daten angezeigt**
  - Branchenscores fehlen und werden kostenlos nur einmalig pro Jahr auf Anfrage postalisch mitgeteilt
  - Gerade die Branchenscores sind entscheidend, jedoch hier keine durchgehende Kontrolle möglich

- **Dienst der SCHUFA kommt dem Online Privacy Service jedoch näher!**

Aktuelle Situation
→ SCHUFA (2/3)

- **Gesamtansicht der SCHUFA-Auskunft**



Meine SCHUFA-Auskunft online

Gesamtansicht

Diese Ansicht stellt Ihnen gesammelt alle SCHUFA-Daten dar, die zu Ihrer Person gespeichert sind.

Daten, die uns ohne Geburtsdatum gemeldet wurden, haben wir besonders gekennzeichnet. Sie erkennen diese Daten am "+"-Zeichen zu Beginn der Kontonummer bzw. des Aktenzeichens.

Druckversion | alle öffnen | alle schließen | Hinweis

Persönliche Daten

SCHUFA-Kundennummer	0123456789
Name	Max Mustermann
Anschrift	Musterstr. 1
	12345 Musterstadt
Geburtsdatum	01.01.1970
Geburtsort	Musterstadt
Zweiter Wohnsitz	

Sonstige, auch frühere Adressen

Aktuelle Situation
→ SCHUFA (3/3)

- **Detailansicht des SCHUFA-Basisscores**

Mein Score

Basisscore: 95,00 % von möglichen 100 %

95,00 % 100 %

Berechnungsdatum: 03.01.2012

Beim SCHUFA-Basisscore handelt es sich um einen von Branchen, Unternehmen und einzelnen Geschäftsarten unabhängigen Orientierungswert, der alle drei Monate neu berechnet wird. Unsere Vertragspartner erhalten zur Unterstützung ihrer Geschäftsentscheidungen in der Regel spezielle branchenspezifische oder individuelle Scores, die durchaus vom Basisscore abweichen können.
Der Basisscore wird anhand moderner mathematisch-statistischer Verfahren erstellt und basiert auf den zu Ihrer Person bei der SCHUFA gespeicherten Daten.

Sie möchten mehr über das Thema Score erfahren? Weitere Informationen haben wir hier für Sie zusammengestellt.

Aktuelle Situation
→ Amazon (1/3)

- **Keine Möglichkeit der Dateneinsicht**

- **Steuerung personalisierter Werbung möglich**
  - Entfernung kürzlich angesehener Artikel
  - Deaktivierung des Verlaufs
  - Abwahl von gekauften Artikeln
  - Deaktivierung personalisierter Werbung

- **Verbesserungen werden dauerhaft serverseitig gespeichert**

- **Deaktivierungen werden im Cookie nur clientseitig gespeichert**

Aktuelle Situation
→ Amazon (2/3)

- **Verwaltung des Verlaufs besuchter Produktseiten auf Amazon**

Nach Kategorie eingrenzen

Alle Kategorien (2)

Bücher (2)

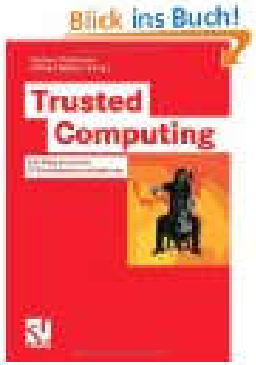
Verlauf besuchter Seiten verwalten

Alle löschen

Klicken Sie hier, um den Verlauf Ihrer besuchten Seiten zu deaktivieren.

Benötigen Sie weitere

Kürzlich angesehen



Trusted Computing: Ein Weg zu neuen IT-Sicherheitsarchitekturen
von Norbert Pohlmann (Dezember 2007)

Preis: EUR 41,95
61 Angebote ab EUR 12,57

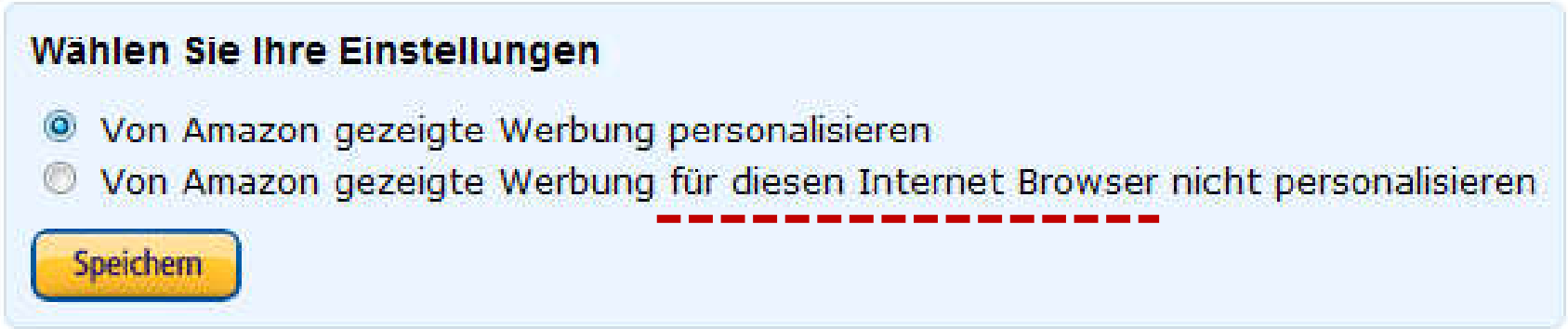
[Diesen Artikel löschen]

Sicher im Internet - Tipps und Tricks für das digitale Leben
von Norbert Pohlmann (12. März 2010)
(4)

Aktuelle Situation
→ Amazon (3/3)

- **Verwaltung der Empfehlungen durch gekaufte Artikel bei Amazon**

- **Deaktivieren der personalisierten Werbung bei Amazon**



Aktuelle Situation
→ Google (1/3)

- **Google hat im Jahr 2007 das Projekt „Data Liberation Front“ gestartet**
  - Daten können seitdem aus jedem Google Dienst einzeln exportiert werden
  - Export erfolgt als Download in offenen Dateiformaten (vCard, JSON)
  - Teilweise können die Daten nicht als Download, sondern zum Beispiel bei GMail nur per POP oder IMAP gesichert werden

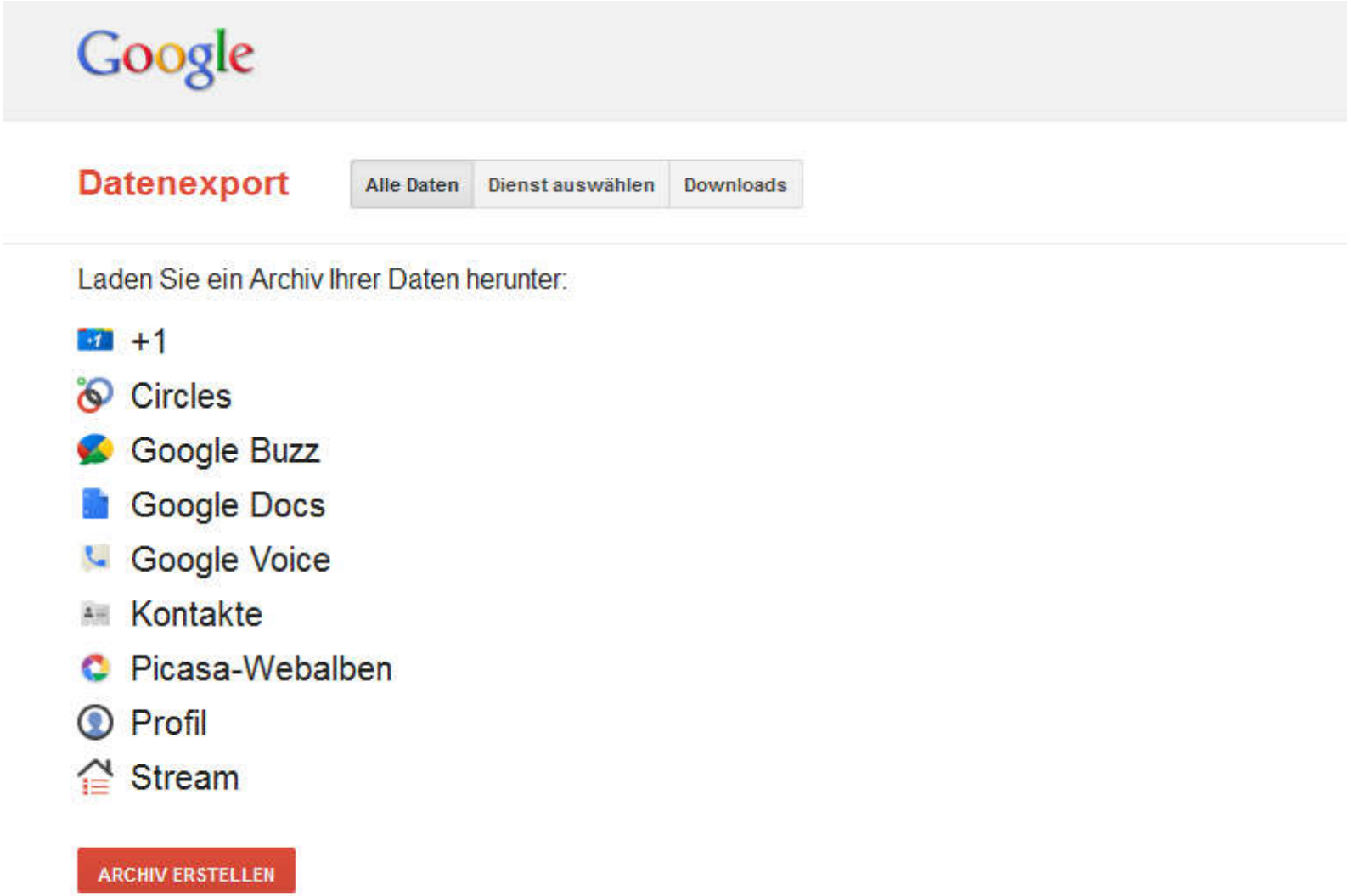
- **Datendownload ist weder einheitlich noch einfach**

- **Mit der Umstellung der Datenschutzbestimmungen zum 01.03.2012 hat Google alle Daten eines Benutzers zusammengeführt**
  - Daten können nun per Google Takeout zusammen in einem Archiv exportiert werden
  - Aktuell werden jedoch nur 9 Internet-Dienste unterstützt,
  - weitere sollen folgen

- **Konfigurieren und Abschalten der personenbezogenen Werbung ist nur bei der Suche und Gmail möglich**

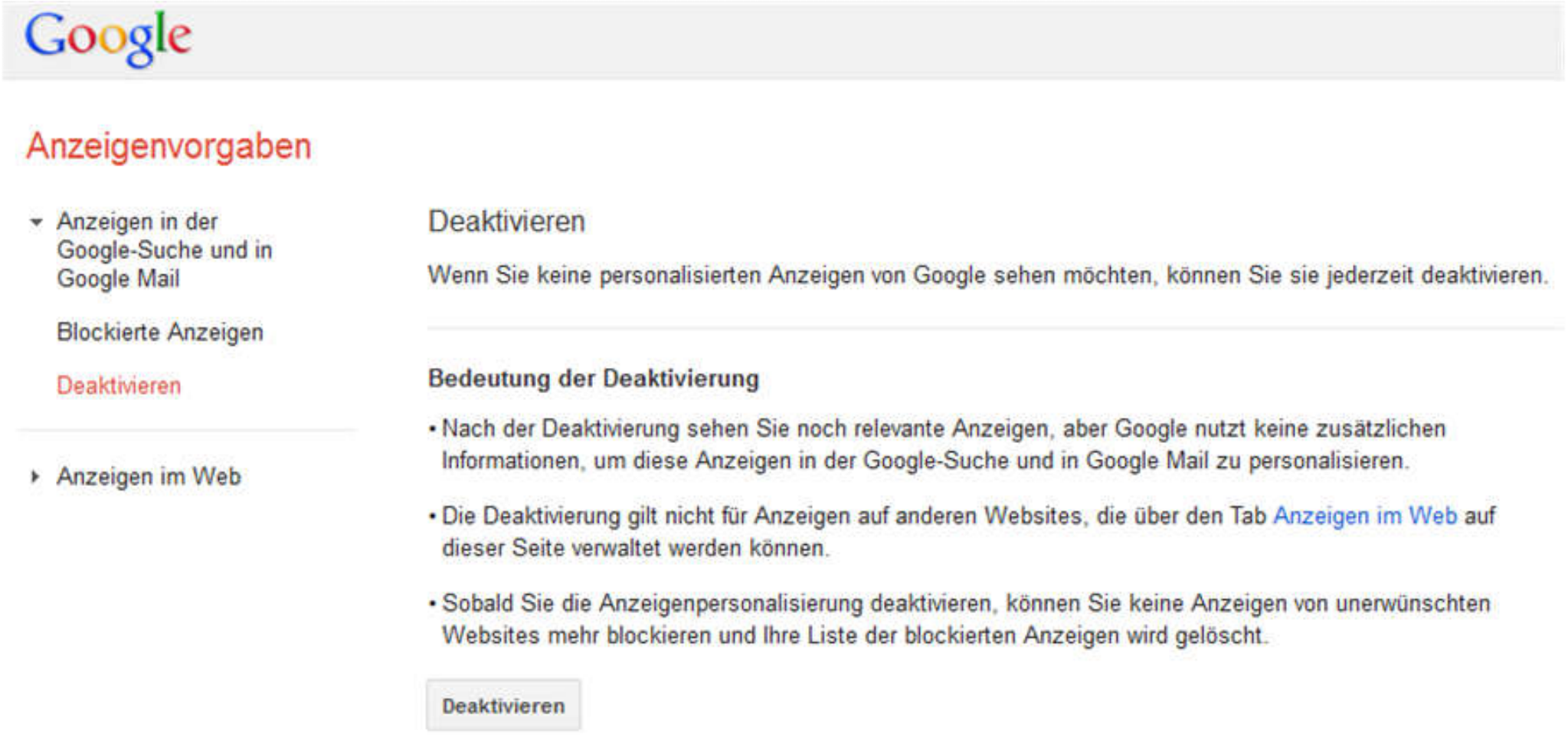
Aktuelle Situation
→ Google (2/3)

- **Datenexport über Google Takeout**



Aktuelle Situation
→ Google (3/3)

- **Deaktivieren der personenbezogenen Werbung bei Google**



Inhalt

- Motivation
- Datenbrief
- Elektronischer Datenbrief / Online Privacy Service
- Bewertung der aktuelle Situation
- **Fazit und Ausblick**

Fazit

- **Die Evaluation zeigt, dass der prinzipielle Bedarf erkannt wird**
  - Jedoch versuchen die Unternehmen die Vorteile für sich zu nutzen
  - Für einen vertrauenswürdigen Umgang brauchen wir deutlich mehr!

- **Online Privacy Service**
  - Zukunftsweisender Lösungsvorschlag für die Anbieter von Onlinediensten
  - Kritikpunkte des Datenbriefes werden adressiert
  - Pragmatischer Ansatz, der Vertrauen erzielen kann

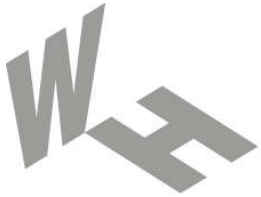
- **Die aktive informationelle Selbstbestimmung im Internet kann so für die Nutzer umgesetzt werden.**

Ausblick
→ Online Privacy Service (OPS)

- **Online Privacy Service muss zu einer Richtlinie weiterentwickelt werden**
  - Betroffene müssen jederzeit bei jedem Dienst standardisiert alle personenbezogenen Daten vollständig, einheitlich, einfach und sicher abrufen, korrigieren und löschen können

- **Der Online Privacy Service könnte im Rahmen der EU-Datenschutz-Grundverordnung in allen Mitgliedstaaten Verbreitung erfahren**
  - Nach Artikel 18, Recht auf Datenübertragbarkeit, Abs. 1, kann die betroffenen Person eine Kopie der verarbeiten Daten in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format verlangen
  - **Wir schlagen mit dem Online Privacy Service eine pragmatische Lösung vor!**

- **Der Online Privacy Service ist der richtiger Weg für eine moderne Gesellschaft und die Gewährleistung der Wahrung der Grundrechte der Bürger**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Der elektronische Datenbrief als aktive informationelle Selbstbestimmung

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann
Maik Heidisch

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
http://www.internet-sicherheit.de

if(is) internet-sicherheit.