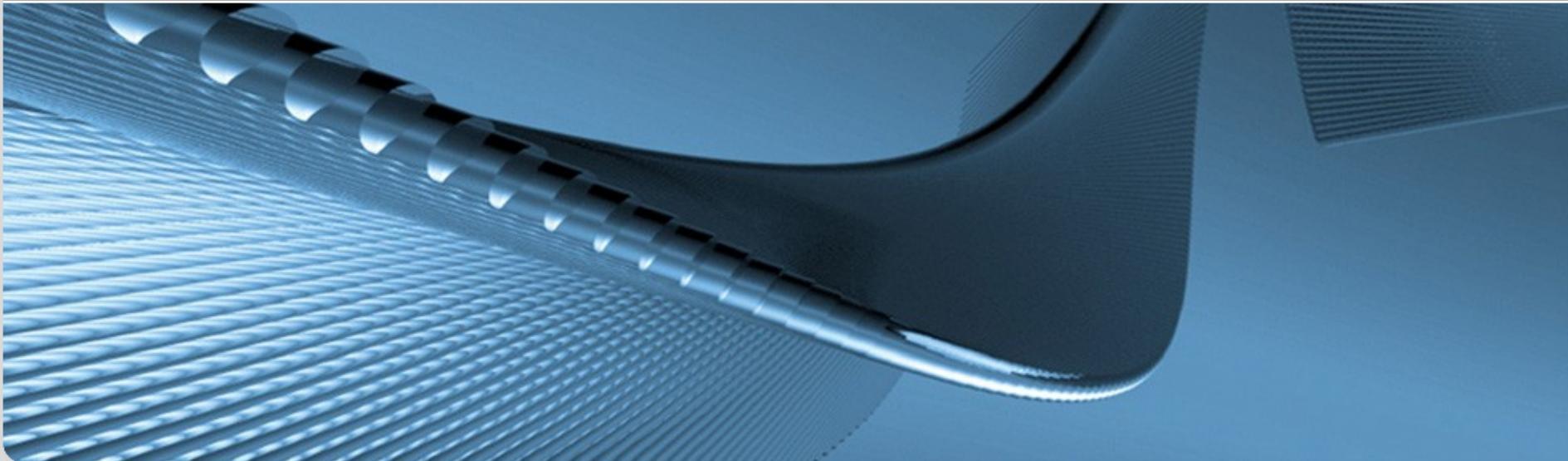


# Datenschutz und Privatheit in vernetzten Informationssystemen

## Kapitel 2: Digitale Identitäten

Erik Buchmann (buchmann@kit.edu)

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“

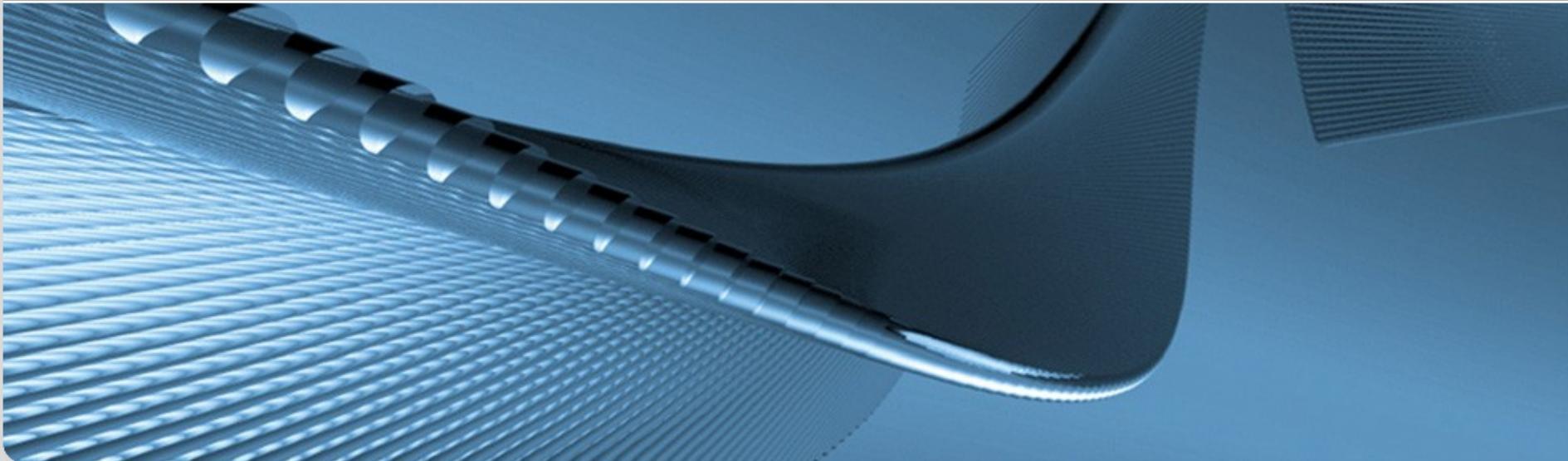


# Inhalte und Lernziele dieses Kapitels

- Digitale Identitäten
- Bedrohungspotential
- Identitätsdiebstahl
- Fallbeispiel: Internet-Suchmaschinen
  
- Lernziele
  - Erkennen Sie, auf welche unterschiedlichen Arten die eigene Identität im Netz repräsentiert sein kann.
  - Sie können die Probleme erklären, die durch eine unkontrollierte Verbreitung dieser (Teil-)Identitäten entstehen können.
  - Sie können Aussagen dazu machen, welche Gefahren für die persönliche Handlungsfreiheit insbesondere durch ein Zusammenführen dieser Teilidentitäten entstehen.

# Die Digitale Identität

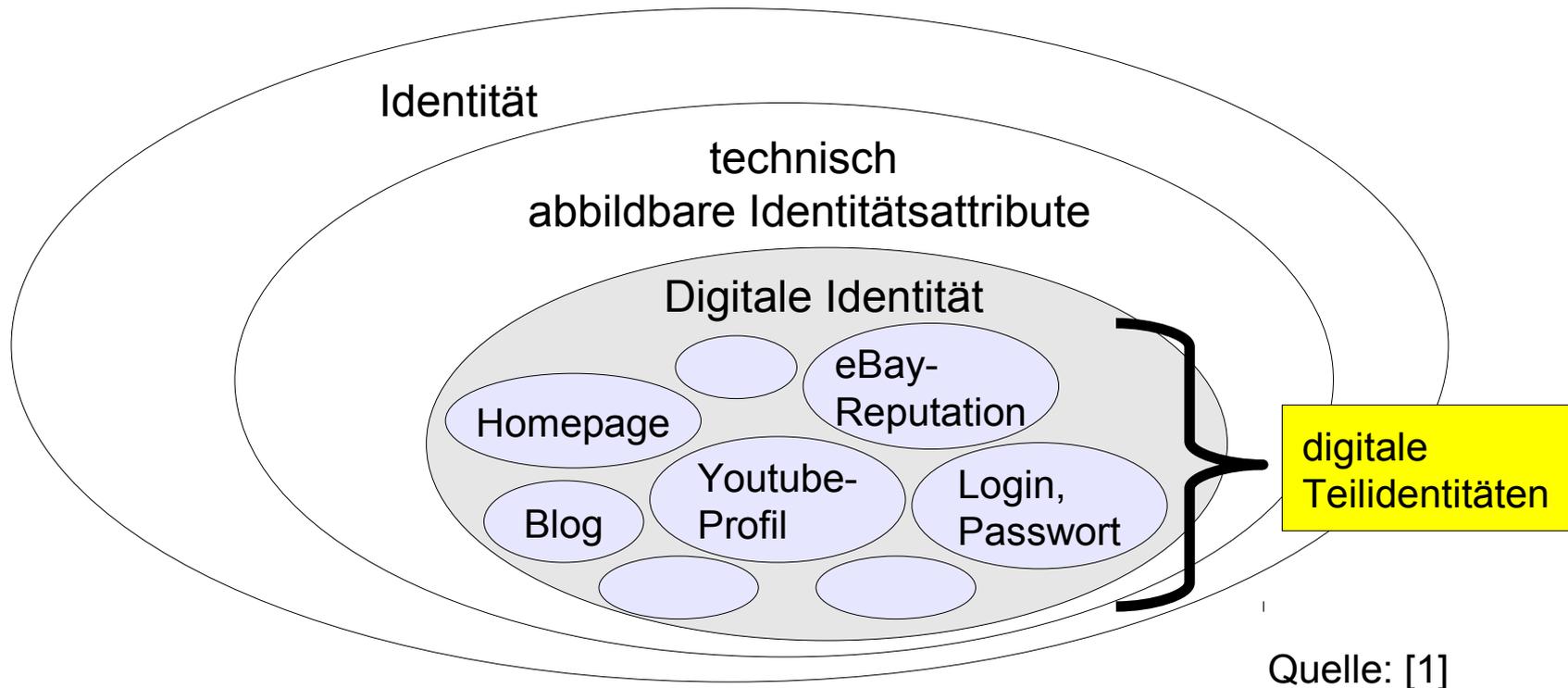
IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



- Definition: “Jede mögliche Form von technisch abgebildeten Daten, die zu einer Person gehören” [1]
  - Daten zur eindeutigen Authentifizierung, z.B. Adresse, Name, biometrische Daten
  - Daten zur pseudonymen Identifizierung, z.B. Login, Passwörter, Nicknames, Foren-Namen
  - Persönliche Merkmale, z.B. Vorlieben, Hobbies, Religion, Lebensumfeld
  - nicht unbedingt von jedem einer Person zuordnbar
    - Beispiel: IP-Adresse ist Teil der digitalen Identität, aber nur vom Internet-Provider zuordnbar

# Übersicht: Identität im Netz

- Digitale Teilidentität: Untermenge der digitalen Identität, die eine Untermenge der abbildbaren Attribute sind
  - viele separate **digitale Teilidentitäten** möglich



# Unterschiedliche digitale Teilidentitäten

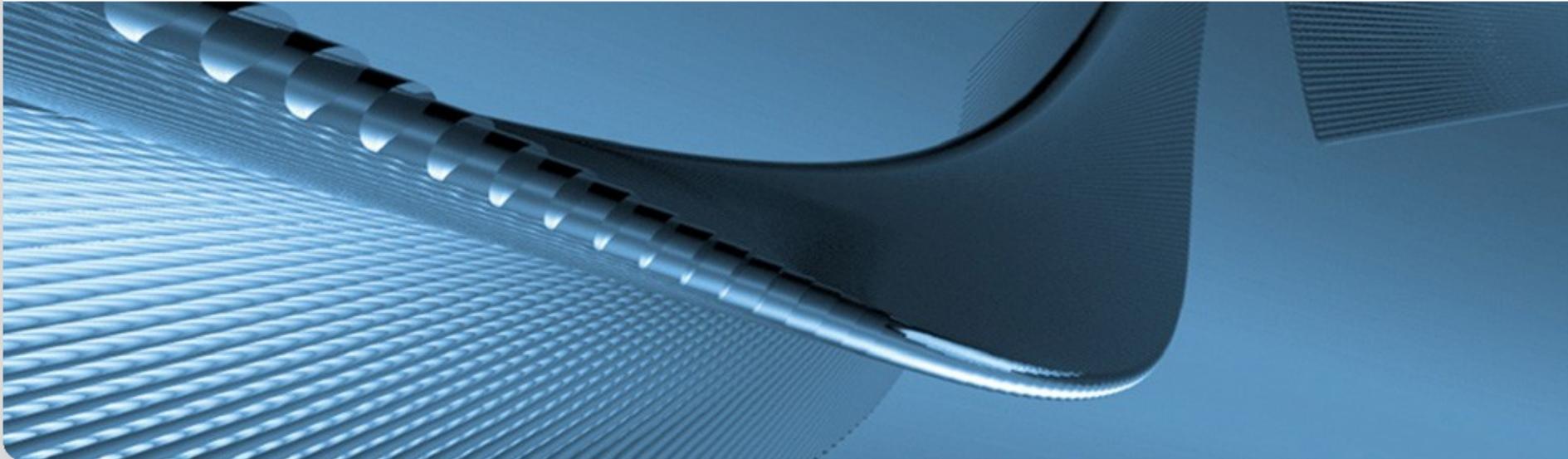
- Datenspuren im täglichen Leben
  - Blogs, Soziale-Netzwerk-Portale, Internet-Communities
  - Finanzamt, Wählerlisten, Anträge bei Behörden
  - Verkehr mit Wirtschaftsunternehmen, Einkäufe im Supermarkt oder Web-Shops
  
- Nicht alle Datenspuren werden wissentlich hinterlassen
  - Was weiß der Supermarkt (Rabatt-System) oder der Mobilfunkprovider (Positionsdaten vom Handy)?  
  
→ durch **Verkettung von Teilidentitäten** Aufbau umfassender Persönlichkeitsprofile möglich!

Weniger relevant für Privatheit	Potentiell gefährlich für die Privatheit
anonym	eindeutig identifizierend
nicht wiedererkennbar	wiedererkennbar
ändert sich im Verborgenen über die Zeit	unveränderlich
leicht änderbar	nicht änderbar
weitergebar / übertragbar	nicht weitergebar/übertragbar
flüchtig	langfristig gespeichert
nur einmal verwendet	häufig wiederverwendet
Authentizität unklar	authentisch / bestätigt durch Dritte
Zugriff anderer nicht möglich bzw. kontrollierbar	Zugriff anderer möglich oder intransparent
ermöglicht keinen direkten Kontakt	ermöglicht unmittelbaren Kontakt
unauffällig/geht in der Masse unter	unnormale oder herausragend
für wenige Teile des eigenen Lebens relevant / als trivial empfunden	betrifft zentrale Bereiche des täglichen Lebens
keine zusätzlichen Informationen enthaltend	enthält für Weitergabe nicht abtrennbare Zusatzinformationen

- Biometrische Merkmale (Fingerabdruck, Gesicht)
  - stabil über die Zeit, kaum änderbar, nicht übertragbar, langfristig speicherbar (Reisepass), häufig wiederverwendet (Passkontrolle), authentisch, andere können darauf zugreifen (sofern nicht verschleiert)
  - **potentiell gefährlich für die Privatheit**
  
- selbstbestimmte Identitätsmerkmale (Login, Passwort)
  - anonym oder pseudonym, leicht änderbar, übertragbar an Dritte, Zugriff anderer nicht möglich, oft nur für unwichtige Teile des pers. Lebens relevant
  - **weniger gefährlich für die Privatheit**

# Bedrohungen durch die Digitale Identität

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



# Probleme mit digitalen (Teil-)Identitäten

- Fehlentscheidungen durch Falschinformationen
- Datenmißbrauch
- Zweitverwertung
- Langfristige Aufbewahrung
- Verknüpfbarkeit
- Öffentliche Zugänglichmachung

*(Anm.: Liste ohne Anspruch auf Vollständigkeit)*

- Offensichtliches Problem: falsche Daten können
  - zu einem falschen Bild in der Öffentlichkeit führen
  - wirtschaftlich schädlich sein, z.B. falsche Schufa-Einträge, falsche Steuer-Berechnung
- Problem
  - Korrektur schwierig umzusetzen, wenn Daten vielfach redundant vorhanden sind
    - Daten in Backups
    - Usenet-Nachrichten, P2P-Dateien vielfach gespiegelt
  - Korrektur schwierig einzufordern, wenn Daten nicht gewerbsmäßig verarbeitet werden, sondern von privaten Anwendern (Wikipedia, Facebook)
  - Datennutzung ist häufig Geschäftsgeheimnis; Fehlentscheidungen für Betroffenen intransparent

- Personenbezogene Daten werden ohne Wissen oder Zustimmung des Betroffenen an Dritte übermittelt
  - einfachste Form: Handel mit Adresslisten
- Ausnahme: einige Arten der Datenübermittlung ohne Wissen und Zustimmung sind gesetzlich legitimiert, z.B.
  - Steuerfahndung
  - polizeiliche Ermittlungen
- Problem
  - unklar, wer Kenntnis von persönlichen Daten hat
  - Verbleib persönlicher Informationen für den Betroffenen nicht nachvollziehbar

- Daten vom Geschäftsbetrieb für andere Zwecke nutzen
  - Data Mining auf Kundendaten
  - Autobahn-Maut (Toll Collect) → Strafverfolgung
  - Handy-Verbindungsdaten → Positionsbestimmung
  - Werbung
- Problem
  - Daten fallen oft unvermeidlich an, z.B. muss Lieferant die Lieferadresse kennen
  - Grenze zwischen legitimer Nutzung für den Geschäftszweck und illegitimer Nutzung oft unklar
  - für den Betroffenen aufgrund fehlender Transparenz oft nicht nachvollziehbar [2]

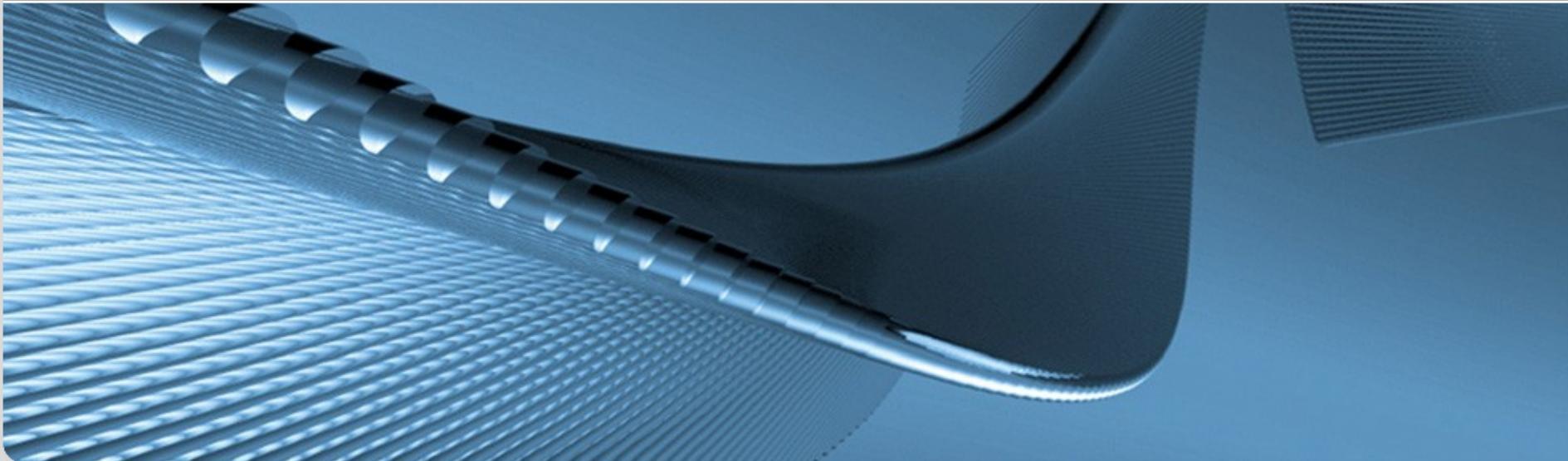
- Zusammenführen von “harmlosen” digitalen Teilidentitäten aus unterschiedlichen Quellen
  - öffentliche Quellen: Telefonbuch, Schufa-Daten, Handelsregister, Liegenschaftsbuch, etc.
  - nichtöffentlich: Daten aus dem Geschäftsbetrieb, Informationen von Behörden, Banken
- Anreichern von eigenen Daten mit Zusatzinformationen
- Suche nach diskriminierenden Merkmalskombinationen in verlinkten Daten → Rasterfahndung
- Problem
  - Aufbau von komplexen Persönlichkeitsprofilen
  - Fehler in den Daten können zu falschen Schlüssen führen

- Daten können beliebig lange gespeichert werden
- Rekonstruierbarkeit und Nachvollziehbarkeit von Aussagen oder Handlungen wird möglich
- Anmerkung: schon aus Praktikabilitätsgründen umfasst die Löschpflicht des BDSG keine Backups
- Problem
  - Selbstdarstellung in der Vergangenheit kann drastisch von aktuell gewünschter Selbstdarstellung abweichen
    - während der Schulzeit Partylöwe, jetzt Lehre zum Bankkaufmann
  - Kontrollverlust über einmal preisgegebene Daten; was einmal im Internet steht ist 'verbrannt'

- Auch objektive Fakten können zu einer falschen Selbstdarstellung führen
  - Auswahl an Informationen entscheidend, z.B. nur wenig schmeichelhafte oder veraltete Daten
- Selbst-Inszenierung des persönlichen Auftritts und Selbst-Bild sind wichtig, z.B.
  - soziale Kontakte, Selbstwertgefühl
  - Vorstellungsgespräche, Verkaufsgespräche
- Problem
  - auch persönliche Daten, die der Betroffene selbst veröffentlicht hat, sind schützenswert
  - Preisgabe von persönlichen Daten durch Dritte, z.B. Freundeslisten in Web-Communities

# Identitätsdiebstahl

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



- Personenbezogene Daten werden ohne Wissen oder Zustimmung des Betroffenen zu Zwecken gesammelt, gespeichert, verarbeitet oder übermittelt, die
  - den Interessen des Betroffenen zuwiderlaufen, z.B.
    - **Identitätsdiebstahl**
    - Stalking, Mobbing
    - Kreditbetrug
  - aber nicht gesetzlich legitimiert sind, z.B.
    - Steuerfahndung
    - polizeiliche Ermittlungen
- Für den Betroffenen nicht zu verhindern, da ohne Wissen und Zustimmung erfolgt

- *“A fraud committed or attempted using the identifying information of another person without authority.”*  
(Definition der Federal Trade Commission, USA)

- unlegitimierte Nutzung einer fremden Identität
- betrügerischer Vermögensvorteil unter Inkaufnahme von Nachteilen für den “Inhaber” der Identität, Kreditgebern, Händlern etc.

Hoofnagle, Chris Jay, *Identity Theft: Making the Known Unknowns Known*.  
Harvard Journal of Law and Technology, Vol. 21, 2007.

# Identitätsdiebstahl USA 2008

## ■ Zahlen 2008: Data Breach Stats (“Einbruchstatistik”)

	<i># of Breaches</i>	<i># of Consumer Records</i>
Banking/Credit/Financial	78	18,731,947
Business	240	5,886,960
Educational	131	806,142
Government/Military	110	2,954,373
Medical/Healthcare	97	7,311,833
<b>total:</b>	<b>656</b>	<b>35,691,255</b>

- Quelle: <http://www.idtheftcenter.org>, Breach Database  
(Anm.: Zahlen beschreiben nur Verlust von pers. Daten, nicht die Mißbrauchsfälle)

# Identitätsdiebstahl USA 2009

## ■ Zahlen 2009: Data Breach Stats (“Einbruchstatistik”)

	<i># of Breaches</i>	<i># of Consumer Records</i>
Banking/Credit/Financial	57	8,364
Business	208	132,402,177
Educational	78	803,667
Government/Military	90	79,470,963
Medical/Healthcare	65	10,461,818
<b>total:</b>	<b>498</b>	<b>223,146,989</b>

- Quelle: <http://www.idtheftcenter.org>, Breach Database  
(Anm.: Zahlen beschreiben nur Verlust von pers. Daten, nicht die Mißbrauchsfälle)

# Identitätsdiebstahl USA 2010

## ■ Zahlen 2010: Data Breach Stats (“Einbruchstatistik”)

	<i># of Breaches</i>	<i># of Consumer Records</i>
Banking/Credit/Financial	54	4,853,708
Business	279	6,626,435
Educational	65	1,598,266
Government/Military	104	1,214,773
Medical/Healthcare	160	1,874,360
<b>total:</b>	<b>662</b>	<b>16,167,542</b>

- Quelle: <http://www.idtheftcenter.org>, Breach Database  
(Anm.: Zahlen beschreiben nur Verlust von pers. Daten, nicht die Mißbrauchsfälle)

- Zahlen 2011: Data Breach Stats (“Einbruchstatistik”)

	<i># of Breaches</i>	<i># of Consumer Records</i>
Banking/Credit/Financial	28	413,348
Business	198	7,917,907
Educational	59	818,458
Government/Military	48	10,036,657
Medical/Healthcare	86	3,732,071
<b>total:</b>	<b>419</b>	<b>22,918,441</b>

- Quelle: <http://www.idtheftcenter.org>, Breach Database  
(Anm.: Zahlen beschreiben nur Verlust von pers. Daten, nicht die Mißbrauchsfälle)

- Betrug durch Erschleichen von Kreditkartendaten: 17.072 Fälle
  - Zunahme seit 2008 um 68% durch Phishing, Trojaner, etc.
  
- Tatmittel Internet:
  - Betrugsdelikte, insbes. Warenbetrug: 169.743 Fälle
  - Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel: 70.918 Fälle
  - Ausspähen, Abfangen von Daten incl. Vorbereitung: 11.491 Fälle
    - davon Ausspähen von Kontodaten durch Phishing: 2923 Fälle
  
- Identitätsdiebstahl:
  - ca. 7000 gemeldete Fälle

- Betrug durch Erschleichen von Zahlungskartendaten:  
19.100 Fälle (2009: 17.072 Fälle)
  - Grund: Zunahme der Internetnutzung und damit mehr Tatgelegenheiten
  
- Tatmittel Internet: 246.607 Fälle
  - Betrugsdelikte, insbes. Warenbetrug:  
182.562 Fälle (2009: 169.743 Fälle)
  - Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel:  
68.528 Fälle (2009: 70.918 Fälle)
  - Ausspähen, Abfangen von Daten incl. Vorbereitung:  
15.190 Fälle (2009: 11.491 Fälle)
  
- Identitätsdiebstahl:
  - 2009 ca. 7000 gemeldete Fälle

\*) Die Statistik für 2011 ist noch nicht heraus

- Physische Ansätze
  - Diebstahl von Brieftaschen, Post aus dem Briefkasten, durchwühlen des Mülls nach Kontoauszügen
- Social Engineering
  - Täuschung und Überredung am Telefon, Erraten von schwachen Passwörtern (Name der Katze)
- Phishing
  - “Wegen *<irgendwas>* braucht *<eine URL, die fast so aussieht wie die die URL Ihrer Bank>* dringend Passwörter, Kontonummer, Pin, Tan und Name”
- Spyware/Viren/Trojaner
  - Mitschneiden der Tastenanschläge, Ausspähen von Passwörtern

# Methoden zum Identitätsdiebstahl (2/2)

- Hacking
  - Einbruch in Firmensysteme, auf denen Kundendaten liegen
- Pharming
  - Angriff eines DNS-Servers, Umleitung von Bank-Webseiten
- Durchforsten des Webs
  - Impressum auf Webseiten, veröffentlichte Lebensläufe auf Bewerbungsportalen, Social-Network-Portalen etc.
- Sorglosigkeit
  - Ausnutzen von versehentlich ins Netz gestellten Daten
- Underground Economy
  - Kauf von Identitätsdaten von Hacker-Portalen
- *(Liste erhebt keinen Anspruch auf Vollständigkeit)*

# Varianten des Identitätsdiebstahls

- Generieren einer (teilweise) künstlichen Identität
  - New Account Fraud
- Übernahme einer bestehenden Identität
  - Account Takeover

- Generieren einer künstlichen Identität
  - echte Daten, um Validierungsverfahren zu täuschen
    - Kontoeröffnung USA: Social Security Number
    - Kontoeröffnung Deutschland: Name, Postanschrift für Schufa-Auskunft
  - künstliche Daten zum Vervollständigen
    - Geschlecht, Alter, Beruf, Einkommen, Familienstand
  - künstliche Daten, um Plausibilität zu erhöhen
    - Vermögenslage (Rechnungen, Hypotheken, Kreditkartenkonten etc.)
    - Lebenslauf

# Erkennung ist schwierig

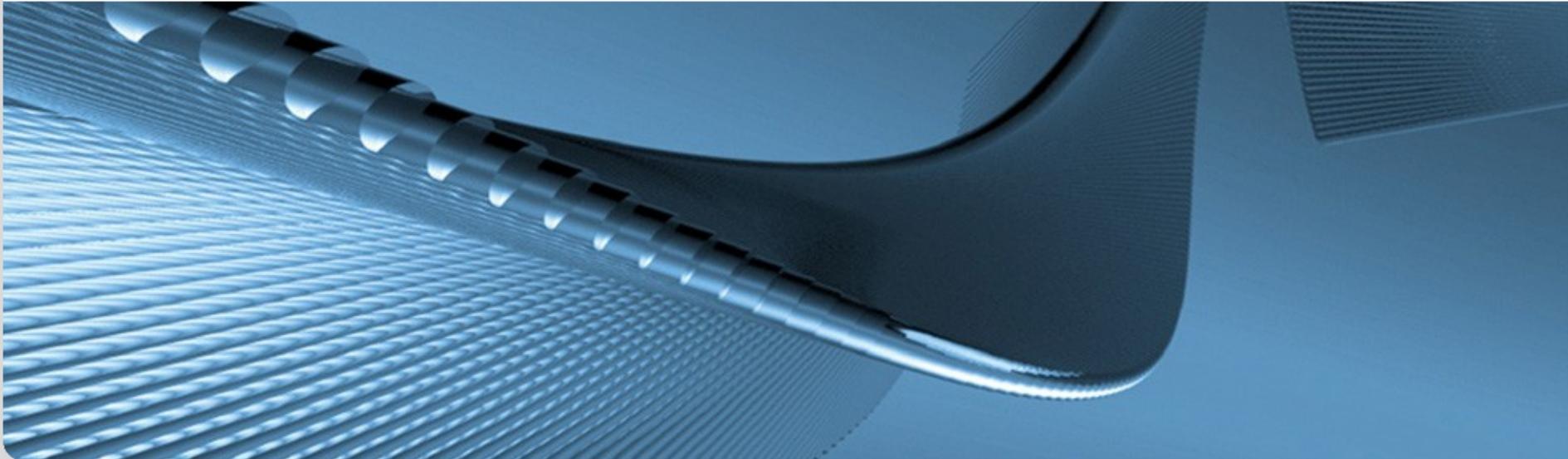
- Künstliche Identitäten bestehen aus Mischung von echten und falschen Daten
- Inhaber der echten Daten erfahren oftmals nur indirekt vom Mißbrauch
  - Korrespondenz, Unterlagen, Mahnungen gehen an den Betrüger
  - Schaden entsteht meist indirekt, z.B. wenn Schufa-Auskunft belastet
- Aus Händler- oder Bankensicht kein Unterschied zwischen flüchtigem Schuldner und gefälschter Identität
  - unklar, ob Betrugsfall oder gewöhnlicher Kreditausfall

- Übernahme einer bestehenden digitalen Identität
  - *Phishing*, gefälschte E-Mails erfragen Kontodaten, eBay-Konten, Kreditkartennummern,  
*www.meinebank.de.pisher.org*
  - *Pharming*, Webbrowser wird durch DNS-Spoofing o.ä. auf manipulierte Webseiten umgeleitet, die eBay- oder Banken-Webseiten gleichen
  - *Malware* auf dem Rechner protokolliert Anmeldeinformationen
  - *Social Engineering*,  
beliebtes Passwort: Name der Freundin,  
beliebte PIN: Geburtsdatum des Kindes

- Account Takeover oft leichter zu erkennen als New Account Fraud
  - die Betroffenen erhalten zumeist Mahnungen, Rechnungen etc.
- gesetzlicher Schutz des Betroffenen
  - Rückbuchung von per Lastschrift eingezogenen Beträgen
  - Stornierung von Kreditkartenrechnungen
  - Strafanzeige gegen Unbekannt

# Fallbeispiel: Identitätsattribute in Suchmaschinen

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



# Suchmaschinen: Google, AOL, MSN und Co.

- Suche übermittelt an Suchmaschinenbetreiber:

Kategorie	Attribute
Suchterme (technisch unvermeidlich)	Aneinanderreihung von Schlüsselworten
Browser-Kommunikation (technisch unvermeidlich)	Zeitstempel, IP, Browser, Betriebssystem, Spracheinstellungen, zuletzt besuchte Seite
Browser-Kommunikation (technisch vermeidlich)	ausgewähltes Suchergebnis, (Implementiert als Redirect)
Zusatzinformationen (vom Nutzer vermeidbar)	Cookie-Informationen, Session-ID
	über JavaScript ermittelte Daten, Verweildauer auf der Seite, Bildschirmauflösung
	Nutzer-ID (z.B. Google-Login, Yahoo-ID)

## ***Mögliche Verkettung dieser Attribute zur Profilbildung***

- Über die **Browser-Kommunikation**, insbes. IP-Adresse
  - dynamische IP-Adressen: überdauern mindestens eine Such-Session
    - Kombination aus Standort des IP-Adressbereichs, Betriebssystem, Sprache, Browser etc. können als Quasi-Identifizierer ausreichen
  - statische IP-Adressen, z.B. Uni-Netz: länger gültig
- Über **Cookies, Session-IDs, Nutzer-Login**
  - Identifiziert einen Browser (und damit oft dessen Benutzer) über lange Zeiträume eindeutig
  - auch bei wechselnder IP-Adresse
- Über die **Suchterme**
  - z.B. Suche nach eigenem Namen, seltene Hobbies
- **Kombinationen** aus allem

- Suchmaschinenanbieter oft Anbieter weiterer Dienste
  - Google: Youtube, Maps, Email, Verzeichnisdienste, Google Docs, Google Earth, News, Usenet
- *separate* digitale Teilidentitäten werden verkettbar
  - über IP-Adresse Nutzerbewegungen über mehrere Dienste hinweg nachvollziehbar
  - oft übergreifendes Login für viele Dienste,
    - Microsoft Passport, Windows Live ID
    - Google Authentication for Web Applications (OAuth)
- Informationen über viele Lebensbereiche
  - Arbeit, Privatleben, Hobbies, Kommunikationspartner etc.

# Haben Suchanfragen Personenbezug?

- kommt ganz drauf an...
  - zur Erinnerung: “...*Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.*”
  - Heute übliche Interpretation: kein Personenbezug, wenn “*für Einzelangaben zu einer Person die Wahrscheinlichkeit, dass diese der Person zugeordnet werden können, so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet.*”

Quelle: Roßnagel, A.; Scholz, P.: Datenschutz durch Anonymität und Pseudonymität, MMR 2000

# Personenbezug von Suchbegriffen

- auch hier: kommt drauf an...
  - “Katzenfutter billig” → nein;
  - “Erik Buchmann Urlaub Italien” → ja
- Personenbezug ist *abhängig von den Benutzereingaben*; nicht ohne weiteres automatisch vom Betreiber entscheidbar!
  - je umfangreicher die Suchhistorie eines Nutzers, desto wahrscheinlicher kommt eine identifizierende Kombination von Identitätsattributen zusammen  
(*Beispiel folgt*)

- Dynamische IP-Adresse
  - eher nicht personenbezogen
    - *Personenbezug erfordert Mithilfe des Kenners der Zuordnungsregel, d.h., Internet Service Provider*
  
- Statische IP-Adresse für festen Rechner
  - Suchmaschinenbetreiber kann Suchanfragen über lange Zeiträume einer Person zuordnen
  - mit zunehmender Zahl der Suchvorgänge steigt Wahrscheinlichkeit, dass sich der Suchende offenbart  
(vgl. vorangegangene Folie)
  - daher: oftmals personenbezogen

Anmerkung: derzeit unterschiedliche Rechtsauffassungen;  
hier vorgestellt wird akutell gängige Praxis – kann sich aber ändern

# Personenbezug von Zusatzinformationen

- Bildschirmauflösung, Sprache, Verweildauer auf der Seite
  - nicht als identifizierendes Merkmal geeignet
  
- Nutzer-Login, Session-ID, Cookie-Informationen
  - Betreiber hat Login, Session-ID bzw. Cookie selbst dem Nutzer zugeordnet
  - daher: oftmals personenbezogen, da *Suchmaschinenbetreiber gleichzeitig Kenner der Zuordnungsregel*

# Aug. 2006: AOL-Datenleck (1/2)

- AOL Research veröffentlicht für Forschung 20 Mio. Suchanfragen von 650.000 Usern, gesammelt über 3 Monate
  - IDs pseudonymisiert, künstl. Schlüssel



User ID	Search Keywords	Date	Website
4417749	numb fingers	2006-03-06 18:35:02	http://irgendwas.de
...	...	...	...

- zwar ist keiner der Datensätze unmittelbar personenbezogen, aber schnell werden einzelne Identitäten und komplette Persönlichkeitsprofile offenbar
- 3 Tage später: Datenbank ist vom Netz, aber schon vielfach in Tauschbörsen kopiert, bis heute verfügbar

# Aug. 2006: AOL-Datenleck (2/2)

- Nutzer 4417749: hunderte Suchanfragen in 3 Monaten
  - “dog urinates on everything”: *Hundebesitzer*
  - “60 single man”: *einsame ältere Frau*
  - “numb fingers”: *körperliche Gebrechen*
  - “homes sold in gwinnett county”: *Wohnung*
  - “xxx Arnold, yyy Arnold”: *suche nach Verwandten*
  - “school supplies for Iraq children”: *karitativ*
  - “best season to visit Italy”: *nächster Urlaub*
  
- identifiziert als Thelma Arnold:  
“*My goodness, its my whole personal life!*”
  - Privat- und Alltagsleben, Ängste, Gebrechen
  - falsches Selbstbild durch Suchanfragen für Freunde

Quelle: <http://www.nytimes.com/2006/08/09/technology/09aol.html>

# Wie handhaben es die Betreiber?

## ■ Google

- nutzt Cookies, verknüpft Daten der Suchmaschine und aller hauseigenen Dienste (Google Docs, Gmail, Google+, Google Analytics)
- Angabe 2009: nach 9 Monaten werden Suchlogs anonymisiert (was immer das heißt)

## ■ Microsoft, AOL, Yahoo

- vergleichbare Praxis der Datensammlung
- Speicherdauer Yahoo, AOL: 6 Monate
- Speicherdauer Microsoft: *“After 18 months, we will completely anonymize all Search queries [...] by irreversibly removing all cross-session identifiers [...] including the full IP address and all cookie IDs.”*  
→ schützt nicht vor persönlichen Suchtermen

# Alternativen existieren

- Es gibt Suchmaschinen, die keine IP-Adressen oder Suchangaben protokollieren



# Zukunft: Collaborative Search Engines (CSE)

- Neuer Trend für Internet-Suche
  - effizient gemeinsam mit Freunden, Kollegen suchen
  - Unterstützen von unerfahrenen Nutzern
  - spannende Suchen und Suchergebnisse weitergeben
  - andere am Alltagsleben teilhaben lassen



Effiziente Suche



Intensive Nutzerinteraktion



Datenschutz?

# Einfachstes Beispiel: Fireball Livesearch\*



The screenshot shows the Fireball Livesearch interface. At the top, there are navigation links: "Profisuche | Livesuche | Hilfe". Below this is the Fireball logo and a search bar. The search bar has a red border and a red arrow button labeled "suche". Above the search bar, there are links for "Web", "Bilder", "Lokale Suche", "Nachrichten", and "Produkte". Below the search bar, there are language options: "deutsch" (highlighted) and "weltweit". A yellow speech bubble points to the search bar with the text "Search engine".

Below the search bar is the "Livesuche" section. It contains the text: "Hier können Sie live sehen, was gerade in FIREBALL gesucht wurde. Sie können Ihre Suchanfrage, um zum jeweiligen Suchergebnis zu gelangen. Die Seite wird alle 10 Sekunden aktualisiert." A yellow speech bubble points to this section with the text "Searches of others".

Below the text are several search results, each with a link and a language indicator: [fortuity](#) - in deutsch, [fortuity](#) - in deutsch, [Partnervermittlung](#) - in deutsch, [jager alpe](#) - in deutsch, [altnuifra](#) - in deutsch, [PowerPoint Präsentations Dienstleister](#) - in allen Sprachen, [holiday check](#) - in deutsch, [altnuifra](#) - in deutsch, [altnuifra](#) - in deutsch, [lidl](#) - in deutsch.

At the bottom of the page, there is a red footer bar with the text: "Ihre Meinung zu Fireball? | Nutzungsordnung | Impressum | Werben auf Fireball | Seite anmelden | Datenschutz | E-Partner | Textversion" and "© 2008 Lycos Europe GmbH".

\*) inzwischen deaktiviert

# Komplexeres Beispiel: SearchTogether

The screenshot shows a web browser window titled "SearchTogether: diabetes (george)". The interface includes a search bar with the text "diabetes friendly recipes", search options like "Standard Search", "Split Search", and "Multi-Engine Search", and a list of search results. Annotations include:

- a**: Points to the search bar area.
- b**: Points to a chat window on the left with messages from "rachel" and "betty".
- c**: Points to the search results list.
- d**: Points to a "Recommendations" section at the bottom left.
- e**: Points to the "Standard Search" button.
- f**: Points to the "Split Search" button.
- g**: Points to the "Multi-Engine Search" button.
- h**: Points to the top right navigation area.
- i**: Points to the "Back", "Comment", and "Recommend" buttons.
- j**: Points to the right sidebar area.

Yellow callout boxes highlight the following features:

- Instant messaging**: Located in a callout box pointing to the chat window (b).
- Searches of others**: Located in a callout box pointing to the chat window (b).
- Search results**: Located in a callout box pointing to the search results list (c).
- Browser**: Located in a callout box pointing to the search results list (c).
- Persistency**: Located in a callout box pointing to the search options (e, f, g).

The search results include:

- VGS - Recipes - American Diabetes Association
- Diabetic Recipes
- Children's Diabetes Foundation - Recipes
- Diabetes-Friendly Holiday Cookie Recipes
- AARP - Segunda Juventud - Diabetes-Friendly Recipes
- AARP - Segunda Juventud - Diabetes-Friendly Recipes
- Book Review: Diabetes Friendly Recipes | Caremark Health

The right sidebar features an advertisement for EXUBERA, a "Reader's Digest" banner, and a "Ho-Ho-Holiday Help!" section with "Diabetes-Friendly Holiday Recipes".

- Gibts sowas?

## Microsoft SearchTogether (Beta)

**April 24, 2008:** SearchTogether is now available for download!  
See below for details on how to install and use SearchTogether.

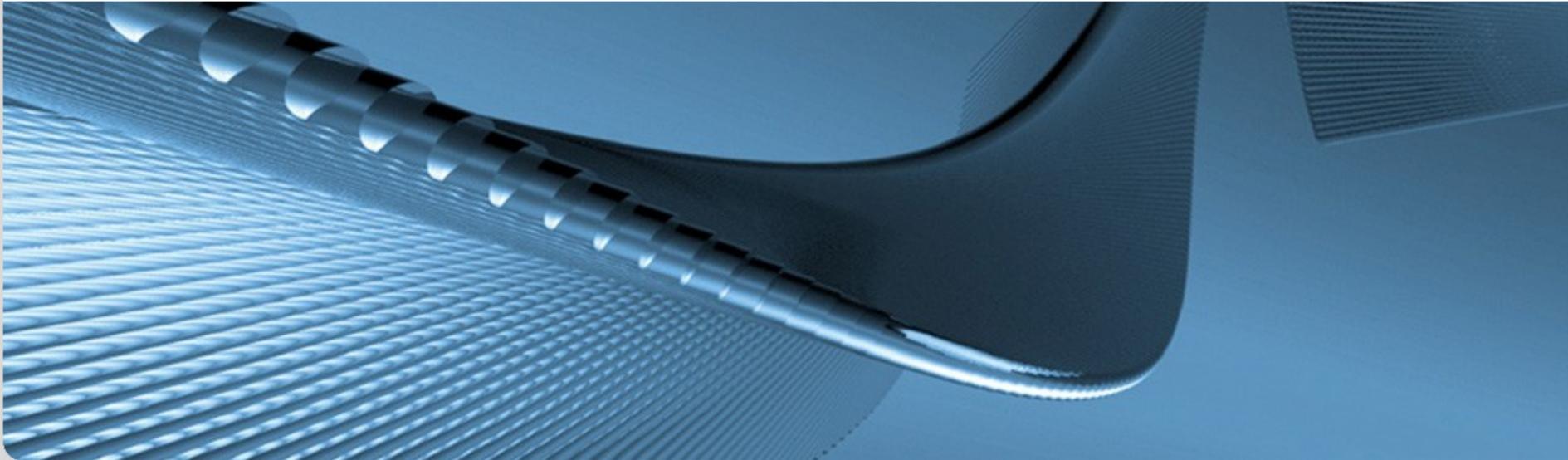
### *Privacy Policy*

SearchTogether allows you to share your web search results and activity with others. When you join a SearchTogether session, your profile, search queries, results, and web site navigation, along with how you use the SearchTogether tool will be sent to Microsoft for research purposes. In addition, this information will be shared with all the people in that session, regardless of when they join. For more information, read our [privacy statement](#).

- Jede CSE-Komponente selbst ist problematisch
  - **Suchmaschine:** Nutzerinteressen, Absichten
  - **Weitergabe von Anfragen, Links:**  
unkontrollierte Verbreitung persönlicher Infos
  - **Kommunikation:** private Gespräche, Kontakte
  - **Speicherung:** Anfragen, angeklickte Links, Kommunikation bleiben für lange Zeit verfügbar
- Verkettung von Informationen potenziert Gefahren
  - “**Speichere** dauerhaft, **wer** sich **wann** für **was** interessiert hat, und **mit wem** er das diskutiert hat.”

# Zusammenfassung

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



- digitale Identitäten als Untermenge aller technisch abbildbaren Attribute mit Personenbezug
- digitale (Teil-)Identitäten sind grundsätzlich bedrohlich, so harmlos sie auch zunächst scheinen mögen
- Identitätsdiebstahl als derzeit größte Bedrohung durch den unbedachten Umgang mit pers. Informationen
- Verkettung digitaler Identitäten führt zu Informationsanreicherung und Profilbildung
- Aktuelles Fallbeispiel: Verkettung in Suchmaschinen

- [1] Verkettung Digitaler Identitäten, *Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein, 2007*
  
- [2] Thorben Burghardt, Erik Buchmann, and Klemens Böhm. *Why Do Privacy-Enhancement Mechanisms Fail, After All?*, W2Trust'08