

Spuren im Internet - und Vorratsdatenspeicherung Theorie und Praxis aus rechtlicher und technischer Sicht.



Der gesetzliche Datenschutz - Recht auf informationelle Selbstbestimmung

- Nach dem BDSG ist die Erhebung, Speicherung, Verarbeitung, Weitergabe und sonstige Nutzung personenbezogener Daten grundsätzlich verboten.

Sie ist nur dann gestattet wenn,

- andere Rechtsvorschriften dies erlauben/gebieten.

- z.B. Meldungen des Arbeitgebers an die Krankenkasse, Datenspeicherung im Einwohnermeldeamt, etc.

- Die Daten zur Abwicklung eines Vertragsverhältnisses verarbeitet werden müssen.
- die betroffene Person einwilligt
- Ein Unternehmen ein berechtigtes Interesse an der Verarbeitung Ihrer Daten hat, das dem Schutzbedürfnis der Person vorrangig ist.
- Die Daten zu dem Zweck verarbeitet werden, zu denen sie ursprünglich erhoben wurden (Zweckbestimmung).
- Angemessene technische und organisatorische Maßnahmen bestehen, um die personenbezogenen Daten zu schützen.

Wen schützt das Bundesdatenschutzgesetz?

- Das BDSG schützt natürliche Personen (also Mitarbeiter, Kunden, Lieferanten, Privatmenschen) vor missbräuchlicher Nutzung ihrer personenbezogene Daten. Juristische Personen (Firmen, Vereine etc.) sind vom BDSG nicht geschützt.
- Bei Weitergabe der Daten an Dritte (Steuerberater, Werbefirma, Lohn- und Gehaltsbüro) bleibt die Verantwortung in den eigenen Händen. Es muss ein Vertrag über den Datenschutz abgeschlossen werden, der dem BDSG entspricht.

Vorratsdatenspeicherung - was wird gespeichert

- Telefonate über Festnetz
- Telefonate über Mobilfunk
- IP-Telefonie
- Versand von SMS
- Versand von Fax
- Versand von E-Mail
- Verbindungen ins Internet

jeweils Sender,
Empfänger mit
Namen, Anschrift,
Provider,
Telefonanbieter,
Verbindungs- oder
Gesprächsdauer, IP-
Adressen,
Funkzellen,
Standort.

Bisher werden keine Inhalte der Kommunikation gespeichert.

Wer darf die gespeicherten Verbindungsdaten einsehen?

- Polizeidienststellen
- Staatsanwaltschaften
- Verfassungsschutzämter
- Bundesnachrichtendienst
- Militärischer Abschirmdienst

Welche Bestandsdaten werden auf Anfrage zur Verfügung gestellt?

- Rufnummern bzw. Mailadresse
- Name des Kunden
- Anschrift des Kunden
- Geburtsdatum des Kunden
- Datum des Vertragsbeginns
- ggf. Anschrift des Festnetzanschlusses

und auf Anfrage spezielle Daten:

- dynamische (also von Fall zu Fall vergebene) IP-Adressen
- Passworte
- PIN und PUK

Privatsphäre und Anonymität - grundsätzliche Überlegungen

Das Internet vergisst nichts. Was Sie heute dort hinterlassen, wird auch noch in zwanzig Jahren und mehr abrufbar sein.

- Welche Informationen gebe ich preis?
- Wem vertraue ich persönliche Informationen an?
- Wie kann ich die Weitergabe von Informationen beeinflussen?

Welche Spuren gibt es:

- Spuren beim Internetprovider
- Spuren beim Webseitenbetreiber
- Spuren in Suchmaschinen
- Spuren beim Online-Banking
- Spuren im Web-Shop
- Spuren in Blogs und Chatrooms
- Spuren durch Emails
- Spuren durch Internetservices

Spuren, die wir unbeabsichtigt hinterlassen

Daten, die der Provider speichert:

Name, Anschrift, Datum & Uhrzeit, IP-Adresse, Zuzungsdauer

Programme, die von kommerziellen Seiten benutzt werden:

- Cookies - auf dem Rechner des Users gespeichert
- Tracking Tools - für Bewegungsprotokoll
- Webbugs oder Webpixel - unsichtbare Einbindung von Fremdanbieter
- PDF- oder Office-Dokumente - Einbinden von Fremdanbietern
- Spyware
- eine Kombination aus diesen Komponenten

Cookies



- speichern Informationen der besuchten Website auf dem eigenen Rechner
- werden von der Website beim nächsten Besuch wieder ausgelesen und eine Wiedererkennung ermöglichen
- Cookies enthalten Informationen über die Benutzung des Webangebots. Loggt der User sich auf einer Seite in seinen Account ein, speichert das Cookie die Anmeldedaten.
- Cookies tragen entscheidend dazu bei, ein Bewegungsprotokoll des Internetnutzers anzulegen.

Tracking Tools



- zeichnen jede Bewegung und jeden Mausklick des Nutzers auf einer Webseite auf
- zeichnen auf, von welcher Seite man gekommen ist und wohin man sie wieder verlässt
- analysieren die Vorlieben und Bedürfnisse des Nutzers und erstellen daraus ein ganz spezifisches Profil
- lesen die eingegebenen Suchbegriffe und die benutzte Suchmaschine aus

Webbugs oder Webpixel

- sind 1x1 Pixel groß und unsichtbar
- stammen generell von Third-Party-Seiten, die Werbeflächen auf der Seite gemietet haben, die der User betritt
- ermöglichen die Erstellung eines Userprofils, obwohl der User diese Third-Party-Seite niemals betreten hat, weil er davon nichts weiß
- gern eingesetzt werden auch Minilinks mit dem Hinweis „Click me“ die optisch zum Seiteninhalt zu gehören scheinen
- verwendet z. B. von der Firma „double-click“, die zu Google gehört



Spyware

- häufig von Marketingfirmen und Webseitenbetreibern programmiert
- wird unbemerkt auf dem Rechner des Users installiert oder manchmal auch absichtlich (Toolbars), weil der User nicht über Spyware bescheid weiss
- spioniert den Inhalt der Festplatte des Rechners aus und protokolliert die Rechneraktivitäten
- sendet die Daten an den Betreiber zur Auswertung
- hat häufig Viren im Schlepptau
- wird selten vom Virenschanner gefunden

Spuren, die wir willentlich hinterlassen



Internet Services

Photocomunities

Chatrooms

Blogs

Foren

Newsgroups

Shops

Ebay

Googledienste

Googlemail

Googledesktop

Googleanalytics etc.

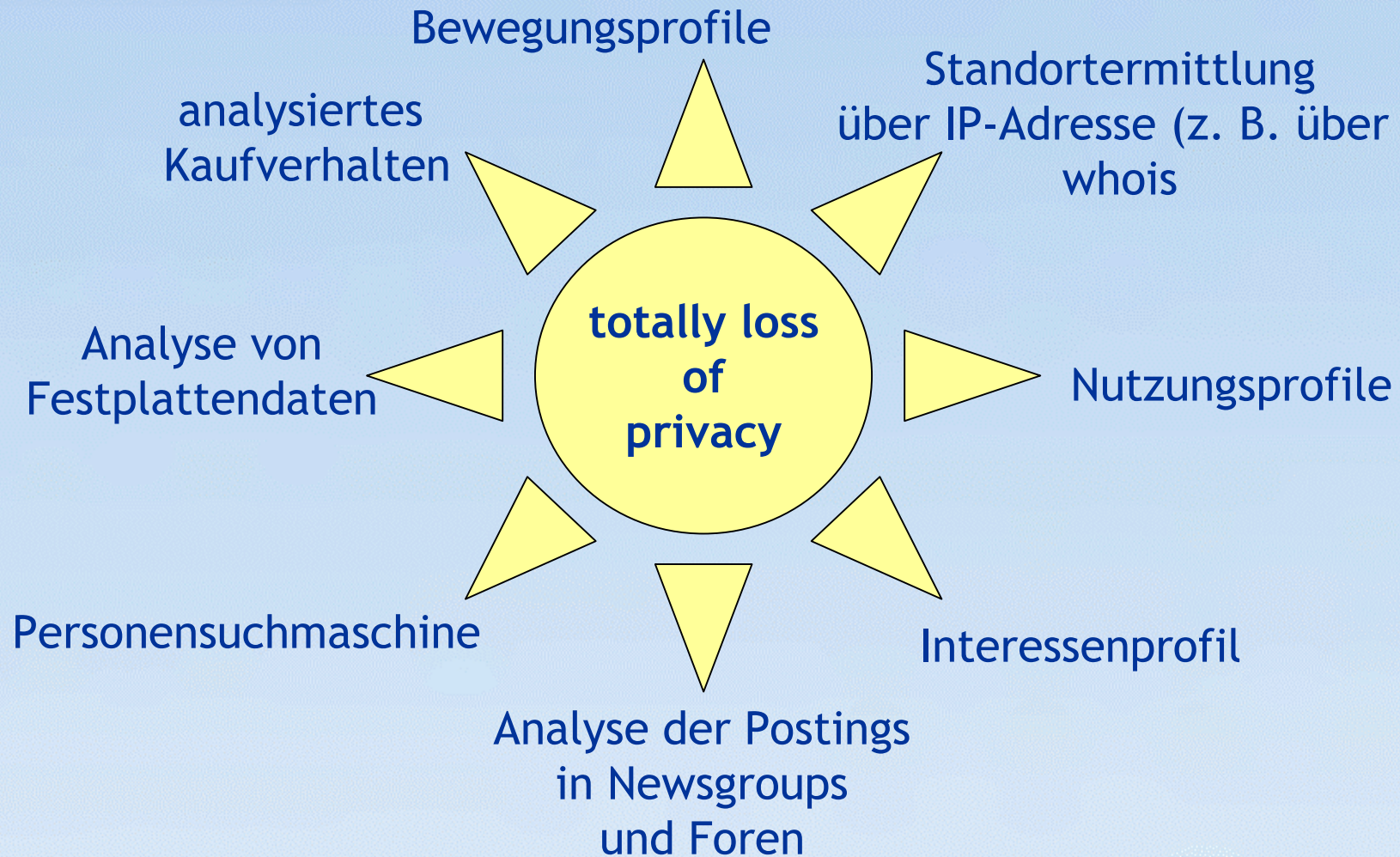
Yahooaccount

Amazon

Banken

und unendlich viel mehr...

Verknüpfung von Daten



Was passiert mit unseren Daten und Profilen

- Speicherung in riesigen Datenbanken zum Zweck der Auswertung
- Auswertung über Knowledge Discovery Programme, um versteckte Informationen über Zielgruppen zu erhalten (Data Mining)
- nutzen der Analyseergebnisse, um den User auf Webseiten gezielt mit Werbung zu versorgen - z. B. durch Bannerwerbung, die explizit nur für diesen User eingeblendet wird
- verkaufen Userdaten an andere Unternehmen
- Staat und Behörden haben ein großes Interesse daran, an diese Daten zu gelangen
- viele der datensammelnden Unternehmen haben ihren Sitz in der USA, somit sind sie nicht an das deutsche Datenschutzgesetz gebunden

Spuren vermeiden

- durch bewusstes und aufmerksames Verhalten im Internet
- durch Absicherung der benutzten Medien
- durch den Verzicht der Preisgabe von persönlichen Daten
- durch Benutzung von lokalen Suchmaschinen
- durch den Verzicht auf Toolbars und Internetdienste wie Google Mail oder Google Desktop etc.

durch lesen der AGBs und Datenschutzerklärungen der Anbieterseiten

Es ist nicht möglich, hinterlassene Spuren vollständig aus dem Netz zu entfernen!

Schutz des eigenen Rechners

- Personalfirewall auf dem Rechner benutzen
- aktuellen Virenschutz verwenden
- Spyblocker einsetzen
- wenn möglich zusätzliche Hardwarefirewall verwenden
- nicht als Administrator am Rechner arbeiten
- bei Nichtbenutzung Internetverbindung deaktivieren

Diese Schutzmaßnahmen können nur mit aktueller Software und richtiger Konfiguration funktionieren!

Online Banking

- HBCI Verfahren mit externer Tastatur, Kartenleser und Chipkarten verwenden
- eTAN oder ChipTAN als Alternative
- Software wie Star Money einsetzen, sinnvoll bei mehreren Konten

Amazon und Co.

- gesicherte Verbindung verwenden, wenn angeboten: meist SSL Verschlüsselung
- nur die wirklich notwendigen Daten hinterlassen
- auf Online-Überweisungen über z. B. PayPal komplett verzichten
- wenn möglich, auf Rechnung kaufen - lieber keine Vorkasse leisten
- vom Account ausloggen

Emails

- Wegwerfemailadressen für Anmeldung in Userforen etc. verwenden, bekommt man z. B. bei Hotmail oder Directbox
- bei kritischen Inhalten verschlüsseln mit PGP
- wichtige Dokumente per Post schicken
- niemals Emails von dubiosen Absendern oder mit ungewöhnlichen Betreffs öffnen. Niemals auf darin enthaltene Links klicken, sofort endgültig löschen
- im Mailprogramm nur-Text-Format verwenden oder das automatische Herunterladen von Bildern deaktivieren
- niemals GoogleMail verwenden, Google wertet die Inhalte aller Emails zu Werbezwecken aus



Bitte helfen Sie mit, ein Bewusstsein für den so notwendigen Datenschutz in unserer Gesellschaft zu entwickeln und informieren Sie insbesondere Ihre Kinder über Gefahren im Internet.

Diese Präsentation erhebt keinen Anspruch auf Vollständigkeit, da das Thema noch sehr viel umfangreicher ist.

Quellenangaben:

www.sicherheitskultur.at - Phillip Schaumann, Spezialist für IT und Informationssicherheit

www.data-defenders.de - Hanns Jörg Proenen, zertifizierter Datenschutzbeauftragter

www.datenschutz-bremen.de - Der Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Sven Holst

www.vorratsdatenspeicherung.de - Arbeitskreis Vorratsdatenspeicherung