

1.4 Informationsaustausch

Arbeitsblatt 18 Rechtliche Bestimmungen beim Informationsaustausch in Netzwerken

Beispiele zum Datenschutz

„Laut Wirtschaftswoche sind derzeit rund 2 Millionen Apps auf dem Markt. Dabei hat TÜV Rheinland herausgefunden, dass etwa 40 Prozent dieser Apps die Daten von Smartphones auslesen, ohne dass der User zustimmt oder es überhaupt erfährt. So können zum Beispiel Standortdaten, Passwörter, Telefonlisten oder das Surfverhalten des App-Nutzers unbemerkt gesammelt, ausgewertet und übertragen werden. Auch Kontakte aus dem digitalen Adressbuch, Textnachrichten, Fotos und Videos sind ungeschützt. Das alles läuft unbemerkt im Hintergrund ab. Problemlos können alle vorhandenen Daten direkt an mögliche Werbeanbieter auf der ganzen Welt gesendet werden, das verhindert auch keine Virensoftware. Somit haben Apps häufig ihren zusätzlichen Preis: nämlich die privaten Daten des Users.“

Quelle: TÜV Rheinland; 07.10.2016; <https://www.checkyourapp.de/>

Hinweis: Der private Bereich wird durch das Datenschutzgesetz nicht erfasst. Wenn man aber in einer öffentlichen oder **beruflichen** Funktion einer App den Zugriff auf das Adressbuch gestattet, ist das rechtlich bedenklich. Dann darf man personenbezogene Daten nur auf fremden Servern **speichern**, wenn Standards für den Datenschutz garantiert sind. Einer nicht näher beschriebenen **Verarbeitung** der Daten durch einen Dritten darf man **keinesfalls** zustimmen.

1. Bewerte *kostenlose* Apps im Hinblick auf den Datenschutz.

➔ Halte dich an das Prinzip der _____

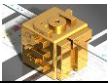
Z. B.: In dem Telefonbuch des Handys sollte ein Name und eine Telefonnummer genügen. Wenn du die E-Mail-Adresse und womöglich auch noch die Postanschrift einträgst, können diese Daten demjenigen, der die Daten erschleicht, umso mehr Geld einbringen.

Man kann hier auch ruhig von *erschleichen* sprechen: Nach PC-Maßstäben sind viele „kostenlose“ Apps *Trojaner*: Wozu braucht z. B. eine Taschenlampen-App Zugriff auf deine Kontaktdaten? Zu der Verwendung der Daten durch den Anbieter findet man oft keine Informationen.

„So hat etwa die derzeit beliebteste Taschenlampen-App von Intellectual Flame nicht nur den Raum mit der Blitz-LED des iPhones erhellt, sondern nebenher gleich mit mindestens fünf Anzeigennetzwerken kommuniziert. Neben iPhone-Modell, iOS-Version, Netzbetreibername und MAC-Adresse des WLAN-Chips übertrug sie dabei auch den Jailbreak-Status...

Nach unseren Beobachtungen verraten vor allem Android-Apps den aktuellen Aufenthaltsort an Werbenetze. Aber auch bei iOS gibt es schwarze Schafe. So erwischten wir die VoIP-App Pinger dabei, wie sie die präzisen GPS-Koordinaten zusammen mit der eindeutigen Seriennummer des iPhones an gleich zwei Werbenetzwerke ... übermittelte. Eine Funktion der App, die diese Informationen im Sinne der Anwender genutzt hätte, konnten wir hingegen nicht entdecken. Das klärt wohl die Frage nach dem Geschäftsmodell des Anbieters, der künftig sogar kostenlose Telefongespräche ins gesamte deutsche Festnetz offerieren will.“ (c't 2012, Heft 7, S. 119)

2. Was ist mit dem *Geschäftsmodell* gemeint?

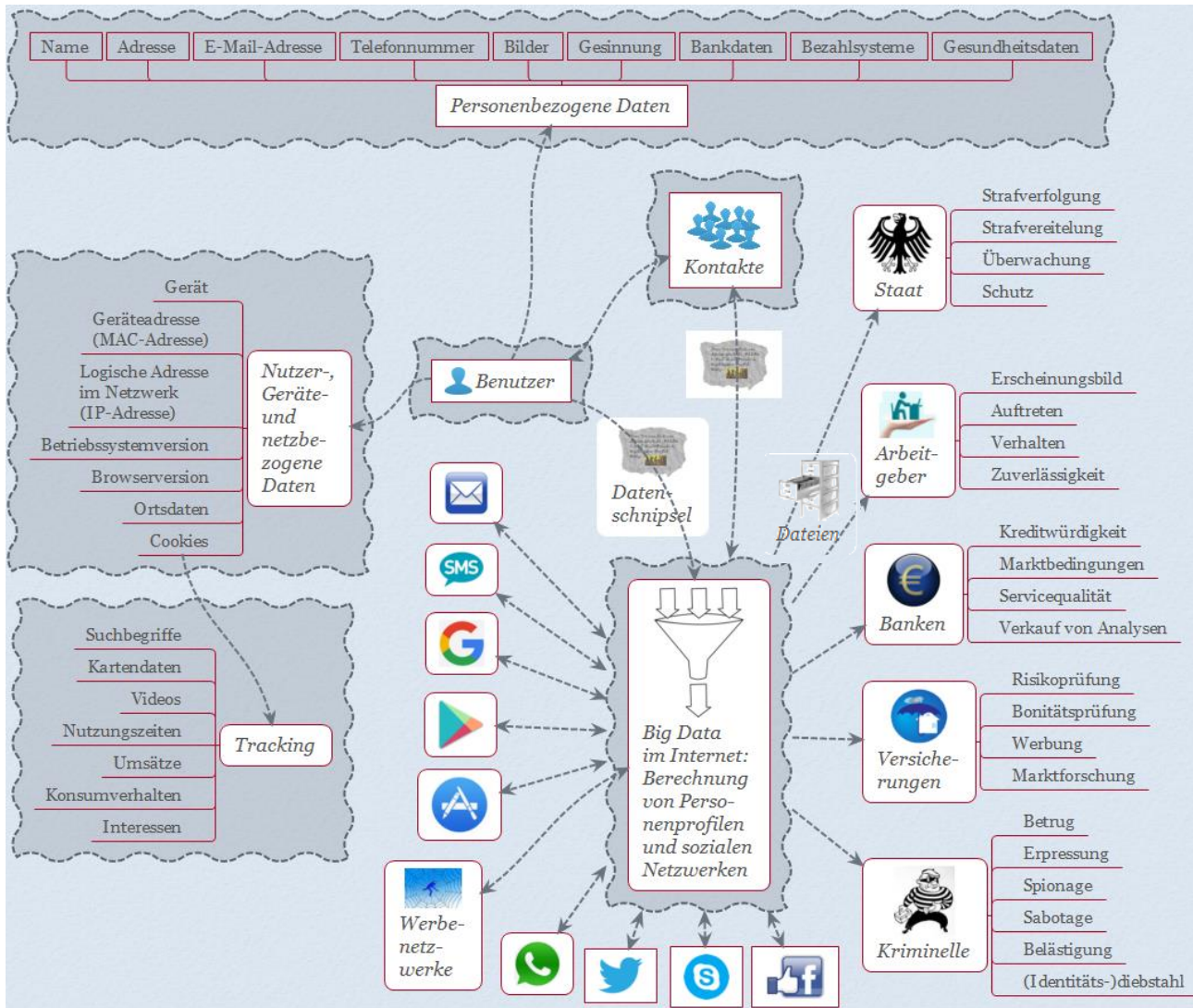


1.4 Informationsaustausch

Arbeitsblatt 18 Rechtliche Bestimmungen beim Informationsaustausch in Netzwerken

„Was kann mir schon passieren? Ich habe nichts zu verbergen.“ Das große Problem sind nicht die einzelnen Datensätze. Vielmehr werden unter dem Stichwort *Big Data* durch die weltweite Vernetzung einzelne Datenschnipsel zu umfangreichen Persönlichkeitsprofilen zusammengestellt.

In der Grafik sind Möglichkeiten zur Gewinnung und Nutzung der Daten von Benutzern sowie mögliche Interessenten daran aufgeführt. Auch wenn man das alles gar nicht auf einen Blick erfassen und begreifen kann, vermittelt die Grafik einen Eindruck für die vielen Möglichkeiten der Verwendung von Daten:



3. Suche in der Grafik einen Begriff, den du kennst. Interpretiere ihn im Gesamtzusammenhang.

Platz für Notizen: