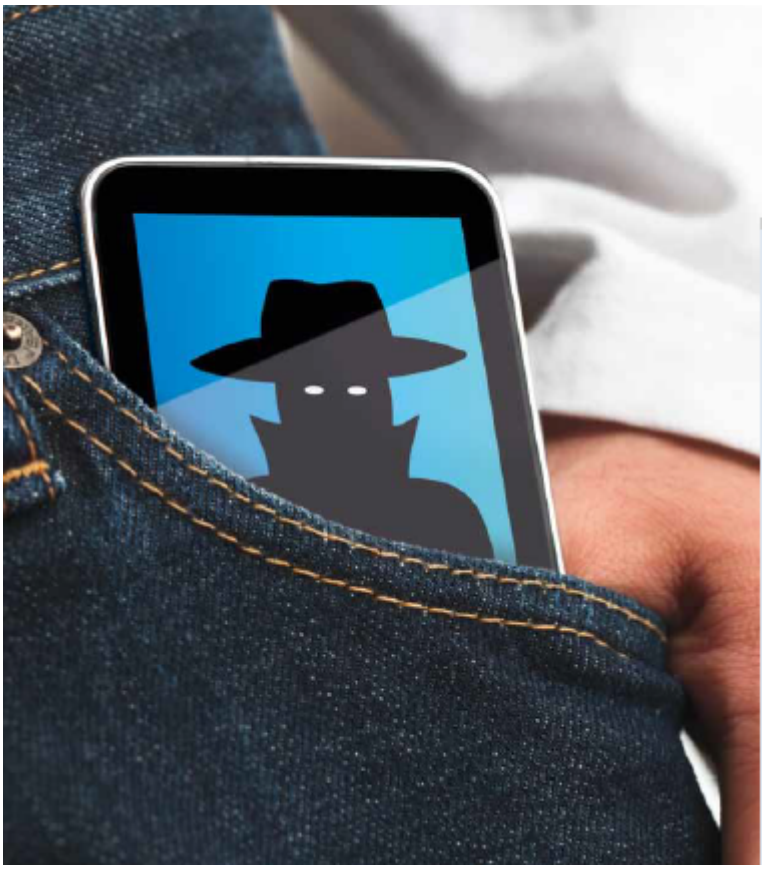
Selbstdatenschutz

Smartphones & Tablets

Smartphones und Apps - die Spitzel in der Hosentasche



Inhalt

Präsentation "Smartphone und Apps - die Spitzel in der Hosentasche"

---

1. Ungewollte Datenzugriffe

Smartphones und Apps sind die Standbeine der mobilen Internet-Nutzung. Sie sind persönliche Begleitgegenstände wie Geldbörsen, Brillen oder Armbanduhren. Wie diese begleiten die Geräte ihre Besitzer auf Schritt und Tritt.

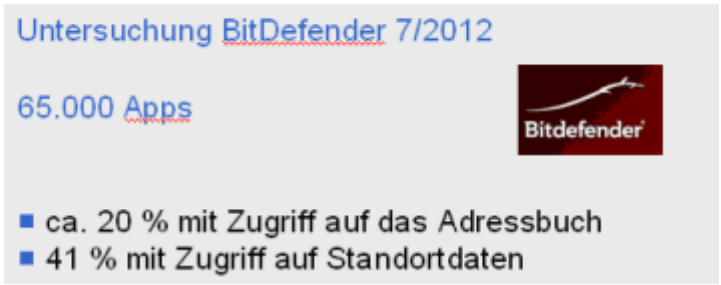
Die digitalen Alleskönner verfügen dabei über ein umfangreiches Wissen über ihre Besitzer und deren soziales Umfeld: Kontaktdaten, Termine, Kommunikations- und Nutzungsverhalten, Aufenthaltsorte, Konsumgewohnheiten, Interessen und Vorlieben. Es lohnt, sich einmal klarzumachen, was Smartphones über ihre Besitzer alles wissen.

Diese Informationen stammen meist aus den so genannten "Apps", die ein Smartphone erst smart werden lassen. Fast eine Milliarde dieser Apps wurde in Deutschland im Jahr 2012 auf mobile Systeme geladen.

Häufig werden diese Daten aber auch ohne Einwilligung der Nutzer erhoben und hinter deren Rücken an Dritte übermittelt und zu teils fragwürdigen Zwecken genutzt.

Verschiedene Untersuchungen zeigen, dass eine Reihe von Apps in einer Weise auf Daten des Smartphones zugreifen, die die Nutzer so nicht erwarten. Etwa, wenn eine Anwendung, die eine bloße Taschenlampenfunktion bietet, auf das Adressbuch, die Telefonliste, den Standort des Nutzers oder die von ihm besuchten Webseiten zugreift - ohne den Nutzer darüber zu informieren oder um Erlaubnis zu fragen.

- **http://blogs.wsj.com/wtk-mobile/**



- **http://s.rlp.de/tpa**

Man sollte also darauf achten, welche Daten eine App verwenden will. Für Smartphones mit dem weit verbreiteten Betriebssystem "Android" lässt sich dies vor dem Download oder spätestens bei der Installation klären, da hier entsprechende Informationsmöglichkeiten bestehen, bzw. der Nutzer darum gebeten wird, den Datenzugriffen zuzustimmen. Bei Geräten mit dem Betriebssystem iOS (iPhone/iPad) erfolgt jeweils eine Nachfrage, wenn auf das Adressbuch oder den Standort zugegriffen werden soll; darüber hinaus kann festgelegt werden welche Apps überhaupt auf Standortdaten zugreifen können sollen.

---

2. Warum passiert das?

Ihre Daten sind Ware und Währung. Im Internet mag vieles kostenlos sein, umsonst ist es nicht. Häufig zahlen Sie mit Ihren Daten. Von Bedeutung sind hier in erster Linie Apps, die kostenlos angeboten werden. Entwicklung und Pflege einer Applikation und deren Vertrieb bringen einen bestimmten Aufwand mit sich. Häufig wird dieser durch Online-Werbung "refinanziert", die mit der Verarbeitung personenbezogener Daten einhergeht. Von zunehmender Bedeutung ist dabei Online-Werbung in Form verhaltensbasierter Werbung, bei der, anders als nach dem Gießkannenprinzip, Werbung ausgerichtet oder passend auf die Interessen und Verhaltensmuster der Nutzer gezielt präsentiert wird. Je gezielter die Werbung auf die Nutzer zugeschnitten ist, desto mehr lässt sich damit verdienen.

Untersuchungen zeigen, dass mit personalisierter Werbung zum Teil mehr als doppelt so viel erlöst werden kann, wie mit unspezifisch verteilter Werbung. Zudem wird Werbung, die mit dem sozialen Umfeld der Nutzer verbunden ist, mehr als drei Mal so häufig wahrgenommen wie neutrale Werbung. Je nach Produktbereich klicken bis mehr als die Hälfte der Nutzerinnen und Nutzer solche Werbung an und bis zu 20 Prozent entscheiden sich in der Folge für das Produkt.

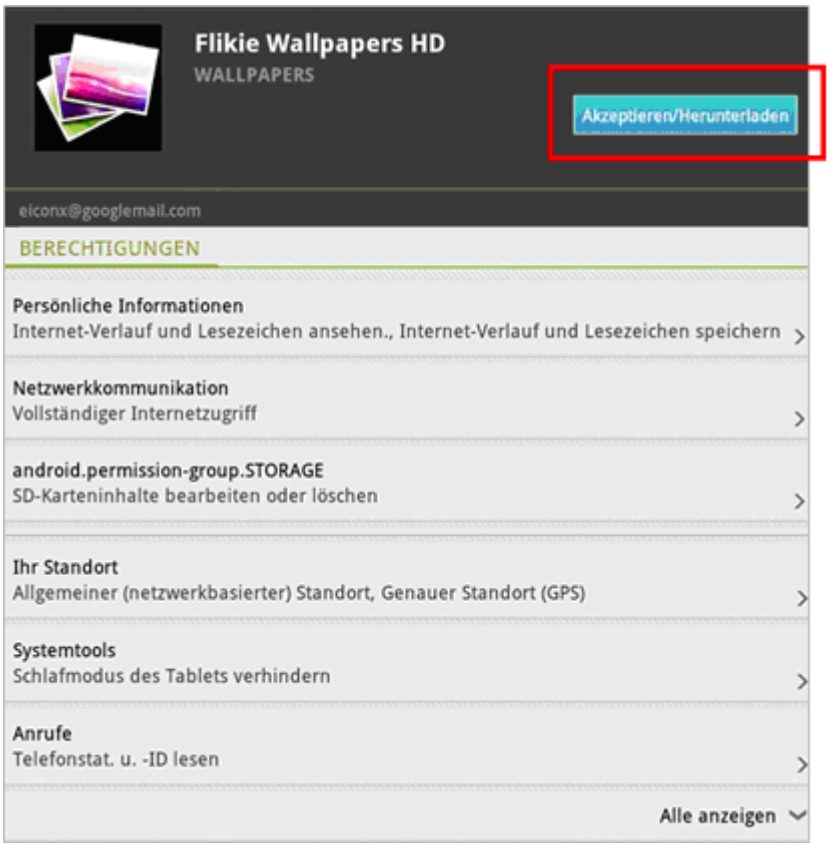
Ziel von Datenerhebungen bei der Online-Werbung ist die Individualisierung von Nutzern, ihre Einordnung in Interessenbereiche (Targeting) und ihre Wiedererkennung bzw. Verfolgbarkeit (Tracking).

---

3. Ungewollte Datenzugriffe erkennen

Auf welche Daten eine App zugreifen möchte, wird für Android-Apps im Rahmen der Installation dargestellt. Wenn Sie eine App installieren wollen, müssen Sie dies bestätigen. Häufig wird jedoch dieser Punkt ohne große Überlegung

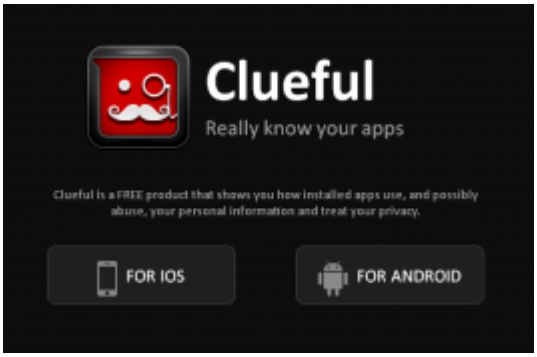
übergangen oder etwaige Bedenken werden zurückgestellt.



Wenn man nachträglich sehen möchte, welche App wie neugierig ist, gibt es hierfür entsprechende Programme, z.B.

LBE Privacy Guard (Android)

Clueful (Android, iOS)

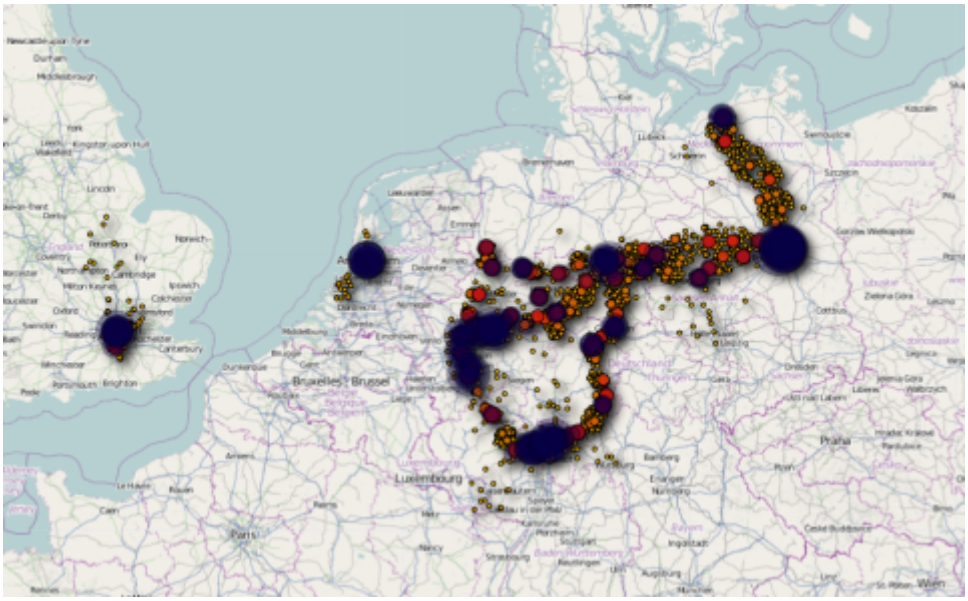


- **http://www.cluefulapp.com/**

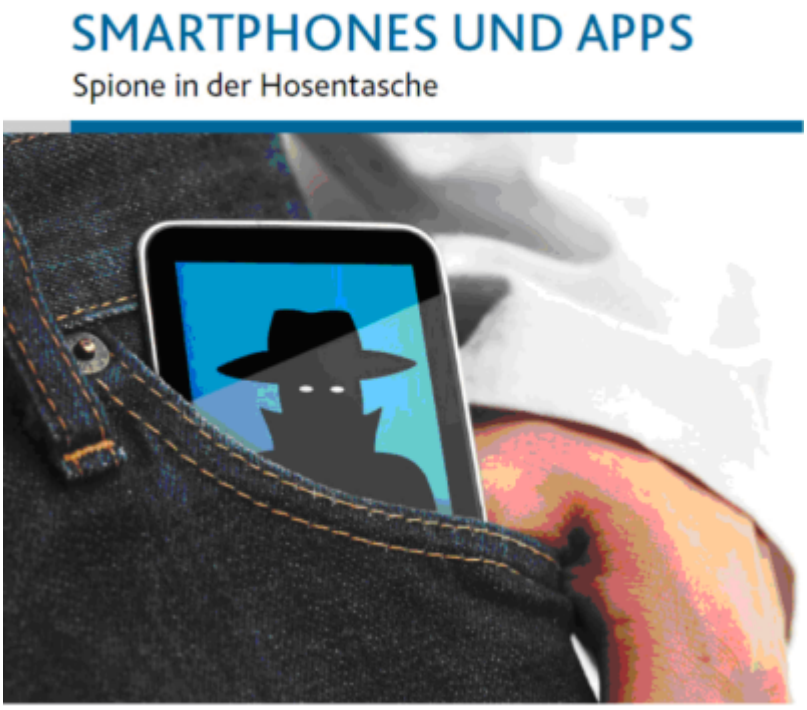
---

4. Wie kann ich ungewollte Datenzugriffe verhindern?

Steuern kann man auch grundsätzlich, ob, wann und wer erfährt, wo man sich gerade befindet. Schließlich muss die GPS- oder WLAN-Funktion des Smartphones ja nicht dauerhaft aktiv sein, und wenn sie abgeschaltet sind, kann auch keine Applikation ungefragt auf Standortdaten zugreifen. Dem ungewollten Auslesen von Standortdaten kann man begegnen, indem man die GPS und WLAN-Funktion deaktiviert, bzw. nur dann einschaltet, wenn sie gebraucht werden.



Welche Möglichkeiten darüber hinaus bestehen, bei den Smartphone Betriebssystemen Android und iOS Datenzugriffe von Apps zu begrenzen, ist in einer **Orientierungshilfe** des Datenschutzbeauftragten dargestellt.



Hinweise zu den Datenschutzeinstellungen von Smartphones mit den Betriebssystemen Android und iOS

---

5. Was kann ich noch zu meinem Schutz tun?

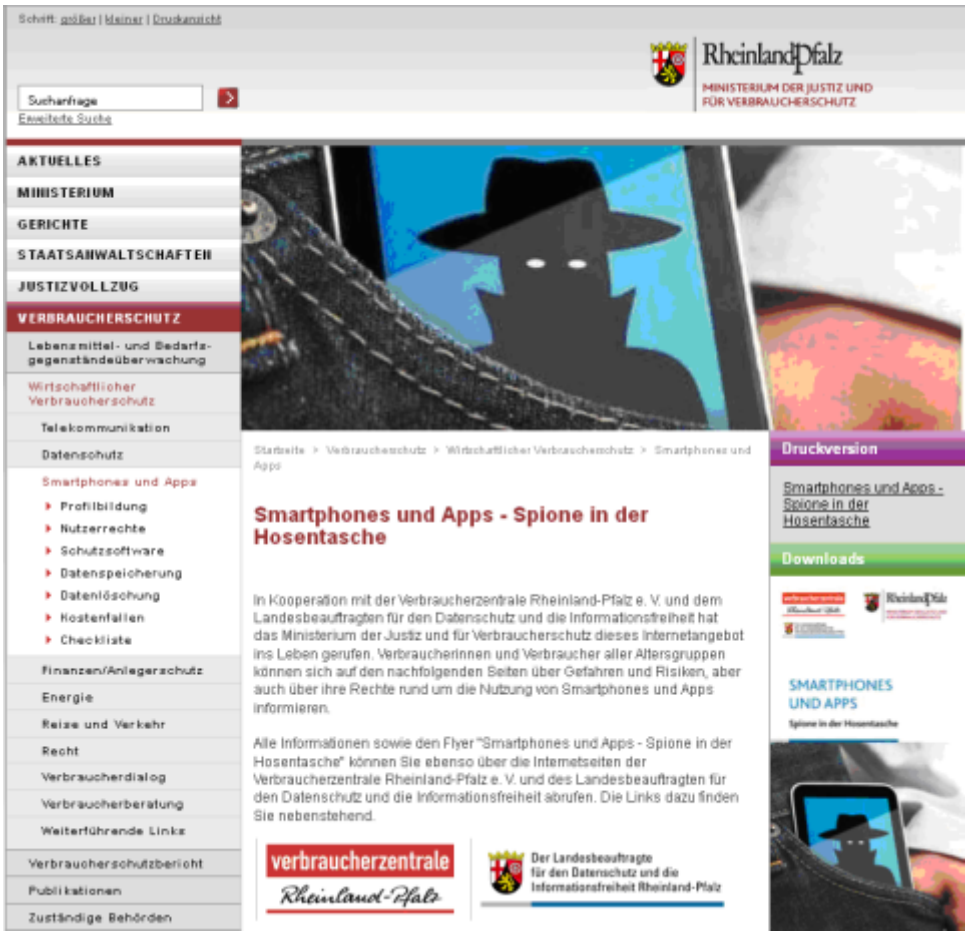
Für manche Daten können Sie über entsprechende Einstellungen festlegen, ob Ihr Smartphone diese an den Hersteller des Gerätes oder an eine App rückmeldet. Da die Geräte in der Standardeinstellung üblicherweise "sehr redselig" sind, sollten Sie Ihr Smartphone gleich bei der Inbetriebnahme dahingehend kontrollieren. Bei der Nutzung von Apps sollten Sie Folgendes beachten:

- Verwenden Sie nur Apps aus sicheren Quellen, also den Softwareportalen der Geräte- bzw. Betriebssystemhersteller.
- Machen Sie sich mit den besonderen Datenschutzbestimmungen einer App vertraut. Beachten Sie, dass diese sich jederzeit ändern können.
- Achten Sie darauf, welche Daten Sie auf Ihrem Smartphone gespeichert und abrufbar haben.
- Schützen Sie Ihre Daten durch Verschlüsselung, Passwort und ggf. die Löschfunktion nach Verlust.
- Löschen Sie Ihre Daten, bevor Sie das Smartphone zur Reparatur geben oder verkaufen.
- Virenschutz und Firewall sind beim Smartphone unbedingt zu empfehlen - auch wenn ihr Schutz nicht dem beim heimischen PC entspricht.
- Führen Sie Sicherheitsupdates durch und aktualisieren Sie regelmäßig das Betriebssystem.
- Sofern Sie wissen, wer Ihre Daten verwaltet, können Sie sich an diesen Anbieter wenden und Auskunft über die gespeicherten Daten fordern.

---

6. Gemeinsame Informationen - Verbraucherschutz

Der Datenschutzbeauftragte hat in Kooperation mit der Verbraucherzentrale Rheinland-Pfalz e. V. und dem Ministerium der Justiz und für Verbraucherschutz ein **Internetangebot** ins Leben gerufen, auf dem sich Verbraucherinnen und Verbraucher über Gefahren und Risiken, aber auch über ihre Rechte rund um die Nutzung von Smartphones und Apps informieren können.



---

7. Weitere Informationen

- Hinweise zu Datenschutzeinstellungen bei **Android**
- Hinweise zu Datenschutzeinstellungen bei **iOS**
- Hinweise zum Anzeigen von **App-Berechtigungen**
