



openHPI – Internet Security Privacy: Summary and Conclusion

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Overview: What Data is Collected? (1/2)

We leave digital traces everywhere:

- Movement data
 - mobile tracking, WLAN, fitness tracker with GPS (manufacturer monitoring), RFID, ...
- Shopping
 - bonus systems, cards, price comparison portals, ...
- Activity and health
 - fitness trackers, smart watches, pedometers in smartphones, ...
- Files and emails
 - various cloud services, emails, ...
- ...

Overview: What Data is Collected? (2/2)

We leave digital traces everywhere:

- ...
- Friends
 - social networks, email providers, VoIP services (Skype, etc.), synchronization of contact data (mobile), ...
- Presence and activities at home:
 - smart home, smart meters, ...
- Interests and Internet use
 - search engines, Facebook, Twitter and other elements on webpages, data retention, ...
- And many more besides:
 - conversations, biometric data, ...

Data Collection- A Critical View (1/2)

Many of the collected data is necessary for the operation of the various services or pleasant for their users

- Mobile tracking is an essential feature of any mobile network
- Storage of customer and transaction data for cashless payments are necessary for security reasons
- Cloud services facilitate backup and restore data as well as collaborate over the Internet
- Social networks enable us to communicate with friends
- ...

Data Collection- A Critical View (2/2)

Often privacy violation first becomes a problem through a correlation of data, e.g.,

- Employer knows salary and address
- Travel agent knows that you go away on weekends
- Bank or online store knows that you purchased a valuable “asset”
- If a gang of thieves have access to all this information, they would know that your home would be an attractive target at the weekend

or

- Pensioner has recently paid for several hospital stays using an EC card from their bank
- Now they want to apply for a credit loan from their bank with a 10 year maturity ...

Central „Data Collection Points" (1/2)

Who has the ability to correlate personal data?

- Large IT companies like Google, Microsoft und Apple
 - i.e., Google has access to
 - search queries on google.com
 - all data on Android phones (synchronization, apps, etc.)
 - watched and favorite videos on YouTube
 - email on Gmail platform
 - usage data from Google Maps
 - data from the Google Drive cloud storage (also Google Docs)
- Internet and telecommunications providers
 - providers have access to all data being sent on the Internet

Central „Data Collection Points" (2/2)

- Secret services and the police
 - can request and/or monitor data from multiple locations (banks, Internet providers, mobile network providers), depending on the national legal situation
- American intelligence agencies (NSA, CIA) and secret services from all US partners (UK, Australia, ...)
 - data from large data collectors in the USA such as VISA, MasterCard, Microsoft, Google, Facebook (many of the large Internet services were developed and promoted in the USA)
 - keywords: PRISM program of the NSA
 - cooperation with German intelligence agency (e.g. XKeyScore program)

Conclusion

- The correlation of actually non-confidential data can lead to a violation of privacy (often not clear which data is relevant for privacy protection...)
- Data minimization where possible: Only share and/or give out the data that are required for a service or operation
- Responsible users must seek **personal compromise** between "payment of usage" of modern technology by giving personal data and protecting their privacy
- Big problem: a lot of data is collected and stored not only nationally (banks, EC card providers, police/ secret services), but also by companies and intelligence agencies in third-party countries
 - differing national legislation on data protection