Privacy in social networks
Social Networks

- "A social network is a social structure made up of a set of social actors (such as individuals or organizations) and a set of the dyadic ties between these actors." – Wikipedia
- "Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively." – Wikipedia
Types of social networks

- Personal Networks
- Status Update Networks
- Location Networks
- Content Sharing Networks
- Shared Interest Networks
The emphasis is on social relationships, for example friendship.

Users share their personal data, relationship status, educational background, employment status, etc. with a (selected) group of people.

Facebook, MySpace, Iwiw
status update networks

- Emphasis is on posting short status updates, to communicate with other users quickly.
- Broadcasting information to the public or a selected group.
- Twitter
Location Networks

- The emphasis is on location–location, user–user and user–location relations.
- Users share their location information, and their opinions about places to the public, or a selected group.
- Foursquare, Loopt
Content Sharing Networks

- Emphasis is on the content.
- Users share multimedia files, and comment on each other’s shares.
- YouTube, Flickr
Shared Interest Networks

- The emphasis is on a common interest of the users, similar hobbies, educational background etc.
- DeviantArt, LinkedIn
Dangers

- Identity theft
- Sexual predators
- Stalking
- Unintentional fame
- Defamation
- Employment
- Surveillance
Identity theft

- Users share their birthday, address, phone number, email address, their mother’s name is not hard to find out ...
- It’s easy to create an account in someone’s name
- Accounts can be hacked, or forgot to log out from.
Lot's of users data
Possibility to create false profiles
MySpace had evicted 90,000 registered sex offenders from its site between 2009 and 2011
Peter Chapman under a false name, added over 3,000 friends and went on to rape and murder a 17 year old girl in 2009
Stalking

- Easy to be a victim of online stalking without even knowing about it
- 63% of Facebook profiles are visible to the public
- AIM permits users to add ‘buddies’ without their knowing, and therefore track when a user is online
Unintentional fame

- Embarrassing pictures or videos getting on Facebook, and then becoming memes.
- For example, a teenager became known as the “Star Wars Kid” when a video about him using a golf club as a light sabre was posted on the internet without his consent.
Defamation

- Social networks can be used to humiliate, and accuse someone, while being anonimous, or hiding behind a fake account.
- On July 24, 2008, British cameraman had posted a fake Facebook page in the name of former business colleague, Mathew Firsht, with whom he had fallen out in 2000. The page claimed that Firsht was homosexual and untrustworthy.
Employers check users social network profiles, looking for discriminating pictures of alkohol or drug consumtion.
  ◦ Can be used positively or negatively

They also check their hired workers’ profiles: „Kimberley Swann was sacked from her position at Ivell Marketing and Logistics Limited after describing her job as ‘boring’.”
The Wall Street Journal found the most popular applications on Facebook were transmitting identifying information about users to advertisers, which is a violation of Facebook's privacy policy.

Electronic footprints, and tracking.
Investigations

- Agents can impersonate a friend, a long lost relative, even a spouse and child.
- With warrant they can ask for data from social sites.
- Alcohol policy violations
- Inappropriate pictures
Collected information

- **User Shares**
  - Age and gender
  - Photos and other media
  - Education, employment history, address
  - Status updates, posts
  - Contacts
  - Interests
  - Geographical location

- **Electronic tracking**
  - Tracking which websites a user has viewed.
  - Storing information associated with specific websites (such as items in a shopping cart).
  - Tracking movement from one website to another.
  - Building a profile around a user.
Information becoming public

- Shared publicly/acidentally
- Shared privately, but to the wrong persons
- Shared by someone else

Hacking
- On August 19, 2013, it was reported that a Facebook user from Palestinian Autonomy Khalil Shreateh found a bug that allowed him to post material to other users' Facebook Walls.
Mixed Public and private profiles

- Possible to attack private information, based on other user’s public informations\(^3\)
  - Privacy attacks using links
  - Privacy attacks using groups
Cookie profiling

- “Cookie profiling, also called web profiling, is the use of persistent or permanent cookies to track a user’s overall activity online” [5]
- Not just on the site, but during the whole browsing
- Even after someone signed out, even if someone just visited the home page [7]
- Facebook has changed as much as they can change with the logout issue. They want to retain the ability to track browsers after logout for safety and spam purposes, and they want to be able to log page requests for performance reasons etc. [8]
Reasons they use it

- "Show what matters to you"
  - They help us know who you are so we can show content that’s most relevant to you, including features, products, and ads.

- Improve your experience
  - They work with Facebook features and help us improve our products and services – so you can do things like see which friends are online in chat, use share buttons, and upload photos.

- Protection and security
  - They help secure Facebook by letting us know if someone tries to access your account or engages in activity that violates our terms.” –Facebook Cookies, Pixels & Similar Technologies
Like and share button cookies are used to monitor which pages, and when were visited.
Can be used to identify someone’s religious affiliations, political views, sexual orientation, and a lot of other things.
Facial recognition

- Facebook’s „Tag Suggestions”
- Enabled by default
- „This feature is a first step in the end of anonymity in the public sphere” – Jimmy Schultz
- „If for any reason someone doesn't want their name to be suggested, they can disable the feature in their Privacy Settings” – Facebook spokesman
Possible defenses

- Not using social networks
- Setting up privacy settings properly
- Choosing friends well
- Deleting all cookies
- Plug-ins:
  - Facebook Privacy List for Adblock Plus
  - Facebook Disconnect
Thank you for your attention

Questions?
References