R.I.P

Steve Jobs
1955-2011
Privacy in Facebook

Franklin Song, 10/6/2011

CPSC 457 Sensitive Information in a Wired World
Taught by Prof. Feigenbaum
Summary

• Conclusion
  • Users, online social networks and application developers, they all have the obligations to protect user personal data. And online social network should only use the data within their websites.
  • It is only user who can grant permissions to third parties to use their personal data, which also means that users should take responsibility on their own.
  • There are also several ways to protect our data from data tracking and aggregating companies.
Online Personal Data

• What is “data”?  
  • “It is what you put in the computer, that goes to the internet and either gets lost or sold. It’s inevitable and a side effect of doing business on the internet.”[1]  
  • Data has business value.

• What is “personal” on the internet?  
  • “It’s nothing. You may think it is, but it isn’t. That’s not just paranoia talking – someone, somewhere has access to your personal data. From the I.T. guys running the bank servers, to the advertisers buying it from your email client, to Facebook opening it up for the world to see.”[1]
Internet Privacy

• “Internet privacy involves the desire or mandate of personal privacy concerning transactions or transmission of data via the Internet. It also involves the exercise of control over the type and amount of information revealed about a person on the Internet and who may access said information.”[3]
  • "Privacy is dead – get over it" – said by a number of experts within the field if Internet security and privacy.
  • “Appeal of online services is to broadcast personal information on purpose.”[3]
• "Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance.” - by security expert Bruce Schneier[4]
  • 87% Americans can be uniquely identified from a birth date, zip code and gender.[6]
  • Chinese human flesh search engine
    • Name, ID, employer, home address, cellphone number, and even profiles of family members.
Privacy

The desire or mandate of personal privacy is important due to the transmission of data via the Internet. It is the person's control over the type and amount of personal information about a person on the Internet and who may access it. "Identity theft" — said by a number of experts within the cybersecurity and privacy.

"It is to broadcast personal information on the Internet that is used to identify and track us by those in power, even if we're aware of surveillance." - by security expert Bruce Schneier.

- 87% Americans can be uniquely identified from a birth date, zip code, and gender.[6]

- Chinese human flesh search engine
  - Name, ID, employer, home address, cellphone number, and even profiles of family members.
is or mandate of personal privacy
oration of data via the Internet. It
type and amount of
on the Internet and who may
ed by a number of experts within
privacy.
broadcast personal information on
those in power, even if we're
surveillance.” - by security
identified from a birth date, zip code
Name, ID, employer, home address, cellphone number, and even profiles
of family members.
or mandate of personal privacy on the Internet. It
and amount of
and who may
of experts within
information on
even if we're
by security
birth date, zip code
on, and even profiles

Name, ID, social security number, and even profiles

C:
8

30

20
Did we pay attention to our internet privacy?

- Facebook for example
  - Did we ever read “Privacy” and “Terms”?

- Did we ever read the terms before click the little check box and hit continue to register on OSN?
Survey

- Knowledge and use of “My privacy” setting feature\(^8\)
  - 289/389 (74%): familiar; 100/389 (26%): not
  - 234/380 (62%): use it; 146/380 (38%): not

- Concerns about Facebook Privacy\(^8\)
  - 12/389 (3.6%) very concerned; 20/389 (6.1%) quite concerned; 104/389 (31.6%) somewhat concerned; 117/329 (35.5%) barely concerned; 76/329 (23%): not
Personal Data in Facebook terms

• “Sharing Your Content and Information”[5]
  • Users own all of the content and information they post on Facebook, and they can control how it is shared through their privacy and application settings.
  • Users grant Facebook to use their content covered by IP rights with permission subject to users’ privacy and application settings.

• “By using or accessing Facebook, you agree to this Statement.”[5]

Notice of Changes
If we make changes to this Privacy Policy we will notify you by publication here and on the Facebook Site Governance Page. If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances. You can make sure that you receive notice directly by liking the Facebook Site Governance Page.
How Facebook protects user privacy

• Privacy Settings
  • Users can manage the privacy of their status updates, photos and information by changing privacy level in the settings.
    • Privacy levels: “everyone”, “friends of friends”, “friends”, “only me”

- How You Connect
  Control how you connect with people you know.
  Edit Settings

- How Tags Work
  Control what happens when friends tag you or your content.
  Edit Settings

- Apps and Websites
  Control what gets shared with apps, games and websites.
  Edit Settings

- Limit the Audience for Past Posts
  Limit the audience for posts you shared with more than friends.
  Manage Past Post Visibility

- Blocked People and Apps
  Manage the people and apps you’ve blocked.
  Manage Blocking

• If you’re under 18
  Privacy Settings
  Since you’re under 18, we take extra steps to protect your information. Learn more
However, your data is still leaking

• By applications you are using

• By third party data tracking and aggregating companies

• Even by your Facebook friends...
Demo

1. Ask for permissions
2. Make an authorization or not
3. Send an access token to app if user makes an authorization
4. You are done...

Demo server & db

facebook

Demo App
Facebook App Permissions

- User profile data access
- User News Feed access
- User actions access
- .......

- Offline access
  - Enables app to perform authorized requests on behalf of the user at ANY TIME.
Who need our data and why

- Online social networks
  - Business purpose, e.g. advertisement
  - Enhance UE (user experience)

- Facebook application developers
  - Business purpose
    - Marketing, e.g. data of users’ friends
  - UE

- Third party data tracking and aggregating companies
  - Business purpose, e.g. www.omniture.com
How do they get our data

- Via cookies[7]

GET ...&g=http%3A//digg.com/users/jdoe...
Host: z.digg.com
Referer: http://digg.com/users/jdoe
Cookie: s_sq=...http%25253A//digg.com/users/jdoe...

- Via referer header[7]

GET /clk;203330889;26770264;z;u=ds&sv1=170988623...
Host: ad.doubleclick.net
Referer: http://www.facebook.com/profile.php?id=123456789&ref=name
Cookie: id=2015bdff9ec|t=1234359834|et=730|cs=7aeppmsks

- Via Get or Post request URL[7]

GET /__utm.gif?__utmhn=twitter.com&utmp=/profile/jdooe
Host: www.google-analytics.com
Referer: http://twitter.com/jdooe
Advantages of utilizing user data

• Better UE
  • e.g. better recommendations, collaborative filtering

  ![Image](image_url)

  I don't understand how facebook chooses the top stories. If you choose for me, please make sure you know me well! Otherwise it's just annoying
  
  Like · Comment · September 22 at 2:49pm · ष

• Better advertisement service
  • e.g. ad in Gmail
Trade-off

- Users might leave if
  - Users consider their privacy to be violated
  - UE drops

- OSN companies will break down if
  - They don’t have enough money
  - No active users

- Online social network companies have rights to use user personal data only within the websites.

- Only users have rights to give permissions to the third-parties, not OSNs.
How to protect our data

• Users
  • Being aware, being sensitive, being careful

• Online social networks
  • Taking responsibility for using users data
  • Launching effective features to protect users’ privacy

• Application developers
  • Do not cheat users

• Third party data tracking and aggregating companies
  • ...
How to protect our data cont.

• Blocking Referer headers
  • e.g. Firefox

• Inserting a “#” character before the id field in its Request-URL
  • e.g. Facebook

• Mapping an OSN identifier to a session-specific value
Reference

[1]. “The Facebook Privacy War: What is Personal Data?”
[2]. “Don't Worry about Who's Watching”
[3]. “Wiki: Internet Privacy”
[4]. “The Value of Privacy”
[5]. “Facebook terms”
[6]. “Betrayed by my shadow: Learning data identify via trail matching”
[7]. “On the leakage of personally identifiable information via online social networks”
[8]. “Facebook: Threats to privacy”