Social Networks
Legal framework and Privacy Enhancing Technologies

Kevin Valk
Mark Vijfvinkel

Security Seminar 2014: Privacy

9 May 2014
What is a social network?

- Facebook, Google, Twitter, Whatsapp, etc...
What is a social network?

- Facebook, Google, Twitter, Whatsapp, etc...
- "... is a theoretical concept in the social sciences, particularly sociology and anthropology, referring to a social structure made up of individuals or organizations." – wikipedia, 05-05-2014
What is a social network?

- Facebook, Google, Twitter, Whatsapp, etc...
- "... is a theoretical concept in the social sciences, particularly sociology and anthropology, referring to a social structure made up of individuals or organizations."
  - wikipedia, 05-05-2014
- "SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users."
  - Article 29 Working Party, Opinion on SNS
Some questions for you

• Who has ever, at some point, joined a social network?
Some questions for you

- Who has ever, at some point, joined a social network?
- Is it a public or “private” profile?
Some questions for you

- Who has ever, at some point, joined a social network?
- Is it a public or “private” profile?
- Do you limit what you put online?

MILDLY SLEAZY USES OF FACEBOOK, PART 14:
LOOKING UP SOMEONE’S PROFILE BEFORE INTRODUCING YOURSELF SO YOU KNOW WHICH OF YOUR FAVORITE BANDS TO MENTION

FAVORITE BANDS? HMM...
MAYBE REGINA SPEKTOR OR THE POLYPHONIC SPREE.

WHOA, THOSE ARE TWO OF MY FAVORITES, TOO!
CLARLY, WE SHOULD HAVE SEX.

OKAY! MY FAVORITE POSITION IS THE RETROGRADE WHEELBARROW.

OMGYGOOD, MINE TOO!
Some questions for you

- Who has ever, at some point, joined a social network?
- Is it a public or “private” profile?
- Do you limit what you put online?
- Who segregates between different types of people?
Some questions for you

- Who has ever, at some point, joined a social network?
- Is it a public or “private” profile?
- Do you limit what you put online?
- Who segregates between different types of people?
- Who is aware of your friends privacy settings?
Some questions for you

- Who has ever, at some point, joined a social network?
- Is it a public or “private” profile?
- Do you limit what you put online?
- Who segregates between different types of people?
- Who is aware of your friends privacy settings?
- Who is considering quitting or has quit a social network?
• I do not like pictures of myself online. Then this happened...
Advantages of a social network

Some points (there are lots more)

- Sharing experiences with people you know
- Keeping in touch with friends, family, etc
- Meeting new people
- It is “free”
- Personalised advertisement
Disadvantages of a social network

Some points (there are lots more)

- Sharing experiences with people you do not know
- Sharing experiences with people you know, but maybe some people should not know that experience?
- Data is not necessarily deleted and might haunt you years later
- You “pay” with your personal data...personalized advertisement
Relational privacy

Privacy concerning personal information towards other people

Platform privacy

Privacy concerning personal information towards the social network
Example:

Europe vs Facebook

- 22 complaints against Facebook in 2011, for example...

- Not deleting pokes, tags, posts, chat messages (platform privacy)

- "When you post information on another users profile or comment on another users post, that information will be subject to the other users privacy settings." (relational privacy)

- Face Recognition, generating biometrical data without consent of the user (platform privacy)
Europe vs Facebook

- 22 complaints against Facebook in 2011, for example...
- Not deleting pokes, tags, posts, chat messages (platform privacy)
Europe vs Facebook

- 22 complaints against Facebook in 2011, for example...
- Not deleting pokes, tags, posts, chat messages (platform privacy)
- “When you post information on another users profile or comment on another users post, that information will be subject to the other users privacy settings.” (relational privacy)
Europe vs Facebook

- 22 complaints against Facebook in 2011, for example...
- Not deleting pokes, tags, posts, chat messages (platform privacy)
- “When you post information on another users profile or comment on another users post, that information will be subject to the other users privacy settings.” (relational privacy)
- Face Recognition, generating biometrical data without consent of the user (platform privacy)
Europe vs Facebook

- Tug of war between EU vs Facebook, Irish Data Protection Commissioner and Facebook.

http://europe-v-facebook.org
Europe vs Facebook

- Tug of war between EU vs Facebook, Irish Data Protection Commissioner and Facebook.
- Request for a formal Decision, on 28-08-2013
Europe vs Facebook

- Tug of war between EU vs Facebook, Irish Data Protection Commissioner and Facebook.
- Request for a formal Decision, on 28-08-2013
- 30-09-2013, Facebook’s response published online
Europe vs Facebook

- Tug of war between EU vs Facebook, Irish Data Protection Commissioner and Facebook.
- Request for a formal Decision, on 28-08-2013
- 30-09-2013, Facebook’s response published online
- This is still ongoing and it is an interesting read so do check it out! http://europe-v-facebook.org
Example:

CNIL vs Google

- Commission Nationale de l’Informatique et des Liberts (CNIL)
Example:

**CNIL vs Google**

- Commission Nationale de l’Informatique et des Libertés (CNIL)
- 1st March 2012 Google combined privacy policies of 60 services into 1 policy.

CNIL fined Google a 150,000 € and demanded a link to its website.
CNIL vs Google

- Commission Nationale de l'Informatique et des Liberts (CNIL)
- 1st March 2012 Google combined privacy policies of 60 services into 1 policy.
- Combined user data collected across several services, e.g. YouTube, Gmail, Google+.
CNIL vs Google

- Commission Nationale de l'Informatique et des Liberts (CNIL)
- 1st March 2012 Google combined privacy policies of 60 services into 1 policy.
- Combined user data collected across several services, e.g. YouTube, Gmail, Google+
- No opt out for users
Example:

**CNIL vs Google**

- Commission Nationale de l'Informatique et des Liberts (CNIL)
- 1st March 2012 Google combined privacy policies of 60 services into 1 policy.
- Combined user data collected across several services, e.g. YouTube, Gmail, Google+
- No opt out for users
- Article 29 Working Party carried out an assessment and found shortcomings
Example:

**CNIL vs Google**

- Commission Nationale de l’Informatique et des Libertés (CNIL)
- 1st March 2012 Google combined privacy policies of 60 services into 1 policy.
- Combined user data collected across several services, e.g. YouTube, Gmail, Google+
- No opt out for users
- Article 29 Working Party carried out an assessment and found shortcomings
- CNIL fined Google a 150000€ and demanded a link to its website
To summarise:

- A lot of people use a social network
- Two privacy views, relational privacy and platform privacy
  - Relational privacy, towards other people
  - Platform privacy, towards the social network
- Two cases that deal with privacy problems of social networks
  - Europe vs Facebook both relational and platform
Legal recap

Legal recap

- Definitions
  - Personal Data, Data Subject, Data Processor, Data Processing
  - Data Controller
Legal recap

- Definitions
  - Personal Data, Data Subject, Data Processor, Data Processing
  - Data Controller
- Data Protection Framework, when is data processing OK?
  - Purpose Specification, Use Limitation, etc (OECD guidelines)
  - And you need a ground for processing
Legal recap

- Definitions
  - Personal Data, Data Subject, Data Processor, Data Processing
  - **Data Controller**
- Data Protection Framework, when is data processing OK?
  - Purpose Specification, Use Limitation, etc (OECD guidelines)
  - And you need a ground for processing
- Consent
Legal recap

- Article 29
Legal recap

- Article 29
- Right to be forgotten
  - Only when data is wrong or incomplete
Legal recap

- Article 29
- Right to be forgotten
  - Only when data is wrong or incomplete
- EU Data Protection Regulation
Legal recap

- Article 29
- Right to be forgotten
  - Only when data is wrong or incomplete
- EU Data Protection Regulation
- Right to erasure
  - Much more control for Data Subjects
  - Headaches for Data Controllers
Legal recap

- Article 29
- Right to be forgotten
  - Only when data is wrong or incomplete
- EU Data Protection Regulation
- Right to erasure
  - Much more control for Data Subjects
  - Headaches for Data Controllers
- Still pending
Article 29 working party (29 WP)

- Independent advisory and consultative body
- Frequently release new working papers and opinions
- Coordinates global enforcement of national supervisors
- Example: Policy difference between friends
Relational privacy: Policy difference between friends [7]

- Relational privacy
- Friend posts information about me on a social network
- If his activities are beyond personal or household activity
- He now becomes a data controller
- Else the household exemption holds
Relational privacy: Household Exemption [5]

- Only when purely personal or household activity
- The directive does not apply on the user
- But, consent should still be given!
- Example: Clubbing pictures
Platform privacy: Right to be forgotten [9]

- French roots “le droit a l’oubli” (right of oblivion)
- Google vs Mario Costeja [2]
- Google was not a data controller and data was not
  - Wrong or
  - Incomplete
Platform privacy: Right to erasure [1]

- Article 17 of the new EU Data Protection Regulation
- This your data around the world
- Data subject can request deletion of its own data
- But freedom of expression still holds
Relational/Platform privacy: Consent [6]

- Consent as legal basis for processing personal data must be free, informed and specific
Relational/Platform privacy: Consent [6]

- Consent as legal basis for processing personal data must be free, informed and specific
- Must be given unambiguously
Consent as legal basis for processing personal data must be free, informed and specific

Must be given unambiguously

May be given explicitly or implied
• Consent as legal basis for processing personal data must be free, informed and specific
• Must be given unambiguously
• May be given explicitly or implied
• When implied, no doubt that subject agrees
• Consent as legal basis for processing personal data must be free, informed and specific
• Must be given unambiguously
• May be given explicitly or implied
• When implied, no doubt that subject agrees
• Sensitive data requires explicit consent
Consent as legal basis for processing personal data must be free, informed and specific
- Must be given unambiguously
- May be given explicitly or implied
- When implied, no doubt that subject agrees
- Sensitive data requires explicit consent
- Consent can be withdrawn at any time
• Who has actually read something they consented to?
• Who has actually read something they consented to?
• What are the most interesting things you have found?
Consent: Facebook

- Non-exclusive, transferable, sub-licensable, royalty-free worldwide license to use any IP content posted on or in connection with Facebook.
- Mobile app requests many permissions (camera, SMS, etc)
- Personal data transferred to and processes in the US
- Deleted data can stay up to 90 days in logs/backups/etc
- The danger of shared data
Consent: Twitter

- Account deletion can take up to 30 days
- Collects log data (IP, username, email, perhaps more)
- Log data can stay up to 18 months
- Privacy Policy is a link in the Terms of Service
Consent: Google

- Information we get from your use of our services
  - Gmail messages, G+ profile, photos, videos, browsing history, map searches, docs, or other Google-hosted content [3]
- Location information
- And a lot more!
Summary

- Relational privacy: Policy difference friends
Summary

- Relational privacy: Policy difference friends
- Platform privacy: Right to be forgotten
Summary

- Relational privacy: Policy difference friends
- Platform privacy: Right to be forgotten
- Both: Consent
Summary

- Relational privacy: Policy difference friends
- Platform privacy: Right to be forgotten
- Both: Consent
- Law currently takes a lot of time (Europe vs Facebook)
Summary

- Relational privacy: Policy difference friends
- Platform privacy: Right to be forgotten
- Both: Consent
- Law currently takes a lot of time (Europe vs Facebook)
- Fines are brushed off (150K fine for a multi billion company)
Summary

- Relational privacy: Policy difference friends
- Platform privacy: Right to be forgotten
- Both: Consent
- Law currently takes a lot of time (Europe vs Facebook)
- Fines are brushed off (150K fine for a multi billion company)
- Can we do something with PETs?
Privacy Enhancing Technologies

- Clearly a problem that cannot be solved by legislation alone
- There exist several PETs, we will discuss a few:
  - Distributed SNS (P2P)
  - Privacy Nudges
  - Multi-Party Privacy
  - Sticky policies
Platform privacy: Distributed SNS

- P2P social network (distributed servers)
- Every server can have its own users
- Server can request data from other servers
Example: Diaspora

- Pods can be based anywhere (legal implications)
- Your data stays on the pod
- Open-source & privacy focused (HTTPS, encryption, etc)
- Easy import from other SNS
Example: Diaspora

- Pods can be based anywhere (legal implications)
- Your data stays on the pod
- Open-source & privacy focused (HTTPS, encryption, etc)
- Easy import from other SNS
- Who is thinking of exploring diaspora?

![diapora* logo]

- Research from Carnegie Mellon University
- Can we nudge users to check their behavior?
- Test case on Facebook
- Good results (users changed behavior)
Privacy Nudges: Profile Picture Nudge

- Notice who will see your post
- Random five profile pictures from your audience
Privacy Nudges: Timer Nudge

• Before the user “posts”
• After the user “posts” the timer counts down
• When the timer reaches zero the post is really posted
Privacy Nudges: Sentiment Nudge

- Shows how others could perceive your post
- Uses open-source sentiment analysis module
- 2477 words with rating -5 to +5 (AFINN-111)
• A policy of one person $\neq$ the policy of his friend
Relational privacy: Multi-Party Privacy [10]

- A policy of one person ≠ the policy of his friend
- Remember the Europe vs Facebook example
Relational privacy: Multi-Party Privacy [10]

- A policy of one person ≠ the policy of his friend
- Remember the Europe vs Facebook example
- “The lack of exposure policies in existing social networks is what allows information to be disseminated against a user’s will.”
Relational privacy: Multi-Party Privacy [10]

• A policy of one person ≠ the policy of his friend
• Remember the Europe vs Facebook example
• “The lack of exposure policies in existing social networks is what allows information to be disseminated against a user’s will.”
• Implement an access control framework that enforces “mutual privacy requirements of all users referenced by a piece of data”
How does this work?

- Every user specifies an exposure policy.
Relational privacy: Multi-Party Privacy

How does this work?

- Every user specifies an exposure policy
- For example, Alice specifies that only Alice’s friends can see Alice’s posts

![Venn diagram showing Alice's friends, Bob's friends, and mutual friends.](Diagram.png)
Relational privacy: Multi-Party Privacy

How does this work?

- Every user specifies an exposure policy
- For example, Alice specifies that only Alice’s friends can see Alice’s posts
- Another example, only friends and not family can view pictures posted by Alice’s friends
How does this work?

- Every user specifies an exposure policy
- For example, Alice specifies that only Alice’s friends can see Alice’s posts
- Another example, only friends and not family can view pictures posted by Alice’s friends
- When there is a mismatch, the info is concealed
Some math...

- $P_u(g) = U$, where $P$ is policy of user $u$. Alice on page $g$. Policy is “visible for all users” $U$
Some math...

- \( P_u(g) = U \), where \( P \) is policy of user \( u \) Alice on page \( g \).
  Policy is “visible for all users” \( U \)

- \( V_w(g, i) \subset U \), where \( w \) is user Bob \( i \) is a piece of information.
  Bob’s exposure policy only allows for his friends to see his posts
Some math...

- $P_u(g) = U$, where $P$ is policy of user $u$ Alice on page $g$. Policy is “visible for all users” $U$
- $V_w(g, i) \subseteq U$, where $w$ is user Bob $i$ is a piece of information. Bob’s exposure policy only allows for his friends to see his posts
- $V_w(g, i) = U$, where $w$ is user Carol
Some math...

- $P_u(g) = U$, where $P$ is policy of user $u$ Alice on page $g$. Policy is “visible for all users” $U$
- $V_w(g, i) \subset U$, where $w$ is user Bob $i$ is a piece of information. Bob’s exposure policy only allows for his friends to see his posts
- $V_w(g, i) = U$, where $w$ is user Carol
- Thus, Alice and Carol agree on the users
Some math...

- $P_u(g) = U$, where $P$ is policy of user $u$ Alice on page $g$. Policy is “visible for all users” $U$
- $V_w(g, i) \subseteq U$, where $w$ is user Bob $i$ is a piece of information. Bob’s exposure policy only allows for his friends to see his posts
- $V_w(g, i) = U$, where $w$ is user Carol
- Thus, Alice and Carol agree on the users
- Alice and Bob do not, thus a privacy conflict occurs
Example

This is somewhat similar to how Facebook has implemented tagging notifications. Unfortunately tag is only removed from your own timeline.

Downsides

What happens when the data is not referenced? For example, I post something without tagging...
Platform privacy: Data deletion

- As a user you store data on a social network
Platform privacy: Data deletion

- As a user you store data on a social network
- If you want to delete data, you want to be sure that it is deleted
Platform privacy: Data deletion

- As a user you store data on a social network
- If you want to delete data, you want to be sure that it is deleted
- How to prove that?
Platform privacy: Data deletion

- As a user you store data on a social network
- If you want to delete data, you want to be sure that it is deleted
- How to proof that?
- Bodies could do unannounced checks
Platform privacy: Data deletion

• As a user you store data on a social network
• If you want to delete data, you want to be sure that it is deleted
• How to proof that?
• Bodies could do unannounced checks
• Legal consequences should be severe to have impact
Platform privacy: Data deletion

- As a user you store data on a social network
- If you want to delete data, you want to be sure that it is deleted
- How to proof that?
- Bodies could do unannounced checks
- Legal consequences should be severe to have impact
- **Holy grail:** Proof of data deletion
Platform privacy: Data deletion

- Technically it is difficult
Platform privacy: Data deletion

- Technically it is difficult
- Data might be altered
Platform privacy: Data deletion

- Technically it is difficult
- Data might be altered
- Stored at various locations
Platform privacy: Data deletion

- Technically it is difficult
- Data might be altered
- Stored at various locations
- Proof of something that is not there?
Platform privacy: Sticky policies [8]

A policy that sticks to data, in which the policy describes what processing is allowed or not allowed. Allows users to improve control over their personal data when it travels across multiple parties.
What can be in the policy?

- Use for the data, for example marketing or research
Platform privacy: Sticky policies

What can be in the policy?

- Use for the data, for example marketing or research
- Use of data within a certain platform only
Platform privacy: Sticky policies

What can be in the policy?

- Use for the data, for example marketing or research
- Use of data within a certain platform only
- Allowed third parties, certain processes
Platform privacy: Sticky policies

What can be in the policy?

- Use for the data, for example marketing or research
- Use of data within a certain platform only
- Allowed third parties, certain processes
- Blacklists, notification of disclosure, deletion after a certain time.
Platform privacy: Sticky policies

What can be in the policy?

- Use for the data, for example marketing or research
- Use of data within a certain platform only
- Allowed third parties, certain processes
- Blacklists, notification of disclosure, deletion after a certain time.
- Specification of trusted authorities
Platform privacy: Sticky policies
Platform privacy: Sticky policies
Advantages

- Provides an audit trail for the user and trusted authority in case of violations.
Platform privacy: Sticky policies

Advantages

- Provides an audit trail for the user and trusted authority in case of violations.
- Provides more control by the user on personal data.
Disadvantages

- Promises can be broken. Would this provide enough evidence in court?
Disadvantages

- Promises can be broken. Would this provide enough evidence in court?
- Trusted authority can decrypt the data, so it really needs to be “trusted”.
Disadvantages

- Promises can be broken. Would this provide enough evidence in court?
- Trusted authority can decrypt the data, so it really needs to be “trusted”.
- Seems difficult to implement correctly.
To summarise:

- We have seen four PETs in two privacy settings
To summarise:

- We have seen four PETs in two privacy settings
- P2P networking (Diaspora), Platform privacy
To summarise:

- We have seen four PETs in two privacy settings
- P2P networking (Diaspora), Platform privacy
- Privacy Nudging, Relational privacy
To summarise:

- We have seen four PETs in two privacy settings
- P2P networking (Diaspora), Platform privacy
- Privacy Nudging, Relational privacy
- Multi-Party Privacy, Relational privacy
To summarise:

- We have seen four PETs in two privacy settings
- P2P networking (Diaspora), Platform privacy
- Privacy Nudging, Relational privacy
- Multi-Party Privacy, Relational privacy
- Sticky policies, Platform privacy
Some questions for you

- Who will quit his/her social network?
- Who is considering to quit his/her social network?
- Who will at least the privacy statement from now on?
- Who will review his/her privacy settings?
• We have seen a distinction between platform privacy and relational privacy
Conclusion

- We have seen a distinction between platform privacy and relational privacy
- Relational privacy on the legal side: Policy difference between friends, household exemption and consent
Conclusion

- We have seen a distinction between platform privacy and relational privacy.
- Relational privacy on the legal side: Policy difference between friends, household exemption and consent.
- Platform privacy on the legal side: Right to be forgotten/erasure and consent.
Conclusion

- We have seen a distinction between platform privacy and relational privacy
- Relational privacy on the legal side: Policy difference between friends, household exemption and consent
- Platform privacy on the legal side: Right to be forgotten/erasure and consent
- Platform privacy on the PET side: Distributed SNS (P2P) and Sticky Policies
Conclusion

- We have seen a distinction between platform privacy and relational privacy
- Relational privacy on the legal side: Policy difference between friends, household exemption and consent
- Platform privacy on the legal side: Right to be forgotten/erasure and consent
- Platform privacy on the PET side: Distributed SNS (P2P) and Sticky Policies
- Relational privacy on the PET side: Privacy Nudges and Multi-Party Privacy
However...

Neither the legal side or the PET side can solve this alone, thus a combination of strong PETs with strong enforcement is necessary. But you already knew that :-)

Food for thought...

- Will this work in practice?
- Current business model of social networks?
- Privacy friendly models better?
- Maybe behavioural advertising needs to change?
N. Bhantooa.  
EU Data Protection Regulation - progress towards adoption, December 2013.  

B. Fox.  
EU court: No ’right to be forgotten’ in data rules, June 2013.  

Google.  
Google: Collected information, March 2014.  
C. of Europe.
95/46/ec of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

*Official Journal of the EC, 1995.*


C. of Europe.
Annexes to the impact assessment, 2012.
C. of Europe.  
Handbook on european data protection law.  
2013.  

S. Pearson and D. Allison.
Privacy compliance checking using a model-based approach. 
http://www.igi-global.com/chapter/privacy-compliance-checking-using-model/49283.

J. Rosen.
The Right to Be Forgotten, February 2012. 
K. Thomas, C. Grier, and D. M. Nicol.
http://dx.doi.org/10.1007/978-3-642-14527-8_14.

Privacy nudges for social media: An exploratory facebook study.
http://dl.acm.org/citation.cfm?id=2487788.2488038.