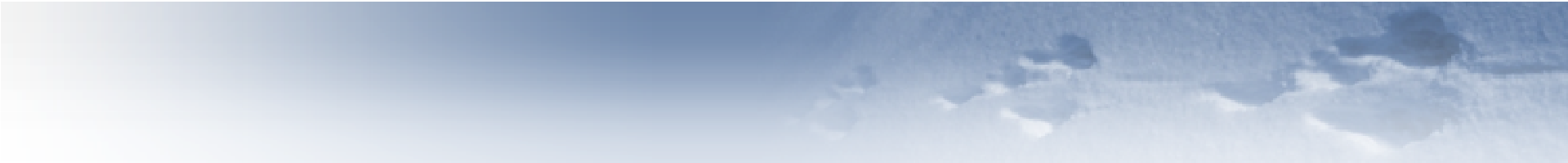# Social Network Services/Sites

- ## ICT mediated services
- ## main features
    - identity ➔ profile page
    - relationship ➔ list of 'connected users' (friends)
    - community ➔ view and traverse others' networks

- ## social functions
- ## privacy challenge
    - sociability: data disclosure
    - privacy: data protection

why are teens on SNS?

- **identity construction**
  - hang out with peers
  - see what is hot and what not

- **social phenomena**
  - social bonding
  - social inclusion
  - "if you're not on Myspace, you don't exist"
  - social pressure
    - "I created an account, because otherwise my friends would have done it for me"
  - social capital

PrimeLife Reference Group Meeting

March 23-24, 2009

people use [Facebook] because it lets them share personal data

James Grimmelmann

PrimeLife Reference Group Meeting   **March 23-24, 2009**

# privacy issues

- **individual level**
  - data disclosure concerning others
    - photos/comments containing others
  - lack of control

- **platform level**
  - profiling by platform providers

- **world**
  - snooping: parents, teachers, bosses, government
  - lock-in and non portability of identities

legal issue

- is profile owner data controller?
  - yes, unless art 3(2)
  - DPD applies
  - (purely personal or
  - household use)
- consequences
  - yes: DPD provisions apply
  - no: no restrictions

- what about public vs. semi-public profiles?
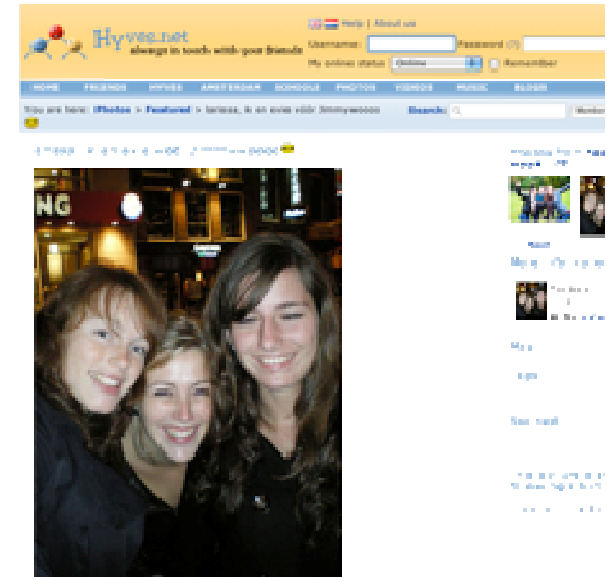
legal issue

- **public profile**
  - DPD applies (Lindqvist case ECJ 6-11-2003 C-101/01,OJ 2004 C7/3)
- **semi-public profile**
  - Dutch court (unpublished):
  - anyone can join group, hence no personal/household use ➜ DPD applies

- **what if proper audience segregation (cocial contexts) and proper access control?**

THE social issue

- ## SNS lack audience segregation
  - friends, friends of friends, rest of the world
  - what about family, colleagues, 'football mates', …

- ## hence
  - schoolyard conversions overheard by everyone:
    - other SNS users
    - platform providers
    - rest of the world

Gov't may track all UK Facebook traffic

Tom Espiner ZDNet.co.uk
Published: 18 Mar 2009 14:25 GMT

The UK government is considering the mass surveillance and retention of all user communications on social-networking sites including Facebook, MySpace, and Bebo.

SNS issues decomposed

identity & relationship

1. Social convergence
2. Sociability paradox
3. False sense of security
4. Eagerness to connect
5. Unauthorised access
6. The user as data controller
7. Instability of social norms
8. Surveillance
9. Simplistic relationship models
10. Denigration
11. Living on the edge
12. Permeability
13. Persistence of identity
14. Stalking

platform provider

15. Panoptic providers
16. Secondary data collection
17. Permeability

transparency

18. It's not what it seems

interoperability

19. Profile non-portability

other

20. Implicit information leaks
21. Advanced monitoring
22. SNS spam
23. SN aggregators
24. Spear phishing using SNSs and SN-specific phishing
25. Profile-squatting and reputation slander through ID theft
26. Bullying
27. Corporate espionagePersistence of identity
28. Stalking

identity & relationship

- **social convergence**
  - roles are context and audience specific. SNS flatten number and types of roles

- **sociability paradox**
  - private profiles enable user control, but make it hard for (new) friends to find you

- **false sense of security**
  - users confuse Gesellschafts for Gemeinschafts

- **eagerness to connect**
  - social inclusion is important, so users accept invitations

identity & relationship

- ## unauthorised access
  - parents, teachers, bosses are not the intended audience, yet they listen in

- ## user as data controller
  - it is you on the photo I posted on my profile (without asking you for permission)

- ## instability of social norms
  - I consider this private information, what do you think?

- ## surveillance
  - users may adapt their behaviour over time as they learn they are being watched

PrimeLife Reference Group Meeting

March 23-24, 2009

identity & relationship

- **simplistic relationship model**
  - friends, what about family, colleagues …
- **denigration**
  - cyberbullying (see Megan Meier case)
- **living on the edge**
  - teens know no fear (until they're 25)
- **permeability**
  - data can be harvested and used elsewhere
- **persistence of identity**
  - it is very difficult to terminate a profile
- **stalking**

platform provider

- **panoptic provider**
  - provider has access to all data, access and networks
- **secondary data use**
  - data is used for profiling and targeted advertisement (and being sold)
- **permeability**
  - data can be harvested and used elsewhere

transparency

- **it's not what it seems**
  - my 'behaviour' not necessarily relates to me

other (selection)

- **profile non-portability**
  - lock-in effect due to inability to move profile and network data from one SNS to the next

- **advanced monitoring**
  - face recognition, EXIF data (pictures), content-based image retrieval, etc allow linking across SNSs

- **implicit information leaks**
  - meta data, relationship data, etc reveal information about user and network

are these the right issues?