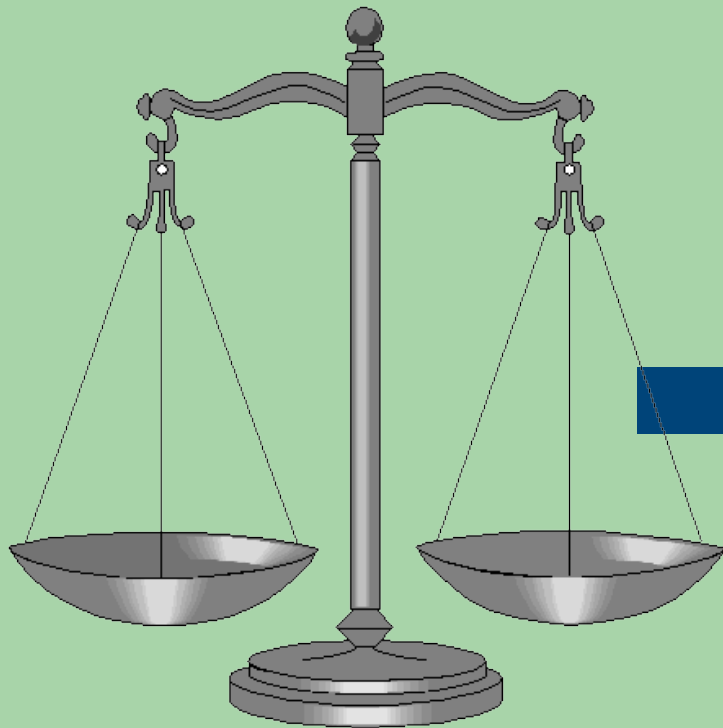


Stalking 2.0

*Ian Brown, Oxford Internet
Institute*

*Lilian Edwards, ILAWS and
Soutgampton*

Chris Marsden, Essex



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!
CLEARLY, WE SHOULD
HAVE SEX.

OKAY! MY FAVORITE
POSITION IS THE
RETROGRADE WHEELBARROW.

OHMYGOD, MINE TOO!



What does one find on Facebook?

- (a) the racial or ethnic origin of the data subject
- (b) his political opinions
- (c) his religious beliefs or other beliefs of a similar nature
- (d) whether he is a member of a trade union
- (e) his physical or mental health or condition
- (f) his sexual life

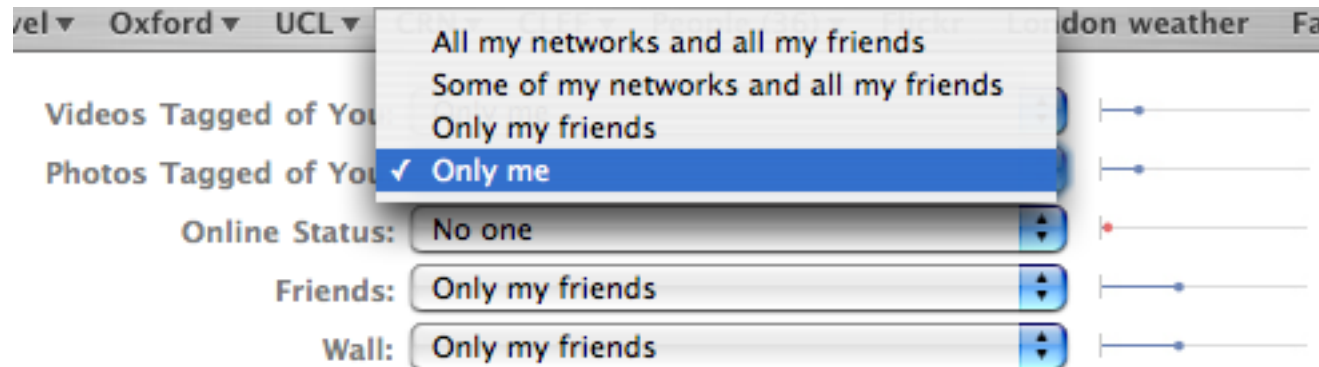
Problems - 1.Tagging

- Should you have a right to control what is “tagged” with your name or identifier?
- Facebook controls who can find “your” tags
- Analogous to concept of structured filing system?



The screenshot shows a Facebook interface. On the left is a navigation sidebar with 'facebook' at the top, a search bar, and a list of applications including Groups, Photos, Events, X Me, Flickr Photos, and LOL Cats. The main content area is titled 'Photos of You Added by Others' and shows 'Photo 11 of 15'. A photo of a man in a light blue t-shirt holding a beer is displayed. A black tag with the name 'Ian Brown' is overlaid on the man's chest. Below the photo is a caption: 'ian with his thimble of beer'. To the right of the caption is a link to the album: 'From the album: "beer fest etc" by Nic Morris'. At the bottom of the photo area, there is a list of tags: 'In this photo: thimble of beer (photos), Ian Brown (photos | remove tag), michael (photos), Dominic Brady'. On the far left, there is a vertical banner for 'Hotels.com' with the text 'Out of this world' and a globe image.

Tag control



- You can control who sees items tagged as you
- Not possible in sites that expose tags to search engines
- PIPL etc.

2- Facebook applications

- Big part of Facebook appeal
- X's consent to FB may reveal personal data about Y also
- See recent "Compare Friends" disclosure for \$\$ scandal.

3-Viral spread`and disclosure

- Apps tend to spam all of your contacts
- Facebook itself encourages you to invite /Friend entire address book
- 2002 directive, 2008 revision

4- Perceptions of privacy

- “Reasonable “ expectations of FB users?
- “Network” disclosure policy?
- School/university networks
- Cf Regional networks (1.2m London members)
- The Oxford proctors and the philosophy student – surveillance using FaceBook (July 07)



Expectation issues

- Whose fault?
- The student because she didn't take appropriate security measures using available tools?
- Oxford's fault for snooping on a "private place"?
- FB's fault because it did not provide the right defaults for a "reasonable expectation of privacy"?
- "Invite-only" networks differ from open networks like FB
- No standardisation of expectations across SNSs eg LJ -> FB
- No standardisation within FB privacy controls.

Oxford: Undergrad Grads Alumni Faculty Staff

UCL: Undergrad Grads Alumni Faculty Staff

- Privacy settings of FB *are* technically sophisticated but the core concept is of "openness" given high school origins

5- User population issues

- If adults rarely take steps to protect their privacy, should we expect teenagers to? Risk awareness; jam today; culture of disclosure. But when FB users grow up..
- What *would* make kids privacy-aware?
- *Wired* July 17 2007 report => “It seems the privacy threat is not so much Big Brother as your mother.” (Otter)
- Some suggestions of default of no spider-able profiles for under 18s on SNSs.
- Some sites much more protective – cf Bebo.

How to further privacy on Facebook and SNSs?

- EU Data Protection law on the whole requires consent to legitimise data collection, processing and transfer
- Is the consent given when signing up for Facebook (and apps) good enough? Informed? “Explicit” for sensitive data?
- Should *current* consent expose users to *future* risks? “The eternal memory of Google”.
- Can T & C which exclude liability for privacy and security breaches be potentially void as unfair consumer terms?
- Some ideas.
 - A legal regime requiring that defaults be provided at the most privacy-friendly setting?
 - Automatic expiration of data?
- Or just let the market decide? Is privacy a bug or a feature ?
- Change society? Out with privacy, in with disclosure and compassion?
- But what will the state, and ID thieves, make meanwhile of the data we give away?