

The auditability of public space –  
*[experiences with Hermes  
situated public displays]*

Alan Dix, Keith Cheverst, Dan Fitton  
and Adrian Friday

[adrian@comp.lancs.ac.uk](mailto:adrian@comp.lancs.ac.uk)

Computing Department,  
Lancaster University, UK.

# Hermes



- 'Connected' post-it notes
  - Situated outside offices
  - 'Owned' by the individual, user participation at each stage
  - Web, email and SMS access
  - 10 units deployed
  - Several cost, safety and disability constraints
  - Longitudinal study (log dating from March 2002)
    - Visibility/**privacy**, remote interaction, appropriation, **security**, calmness/ salience...

# Use and usability

- Messages can be left *for visitors/ passers* by
  - Intentional sharing of context (c.f. post-it)
  - Visible to anyone, but only at your door
  - Use of expressiveness/ ambiguity - subtlety  
*“In big q at post office.. Will be a bit late”*
- And left *by visitors*
  - Can write anonymous messages that are delivered via email/ web (as written)
  - Can authenticate using PIN or iButton to read & leave messages
  - Messages left are intentionally not visible

# Fear and loathing

- Initially, fear that system would lead to string of unpleasant or abusive messages
  - Deliberate ‘low cost of entry’ to use the system (security vs. ease of use)
  - Messages are anonymous by default
  - No limits (e.g. quota, financial) or access controls
  - Yet instances of abuse have been almost non-existent

# Mischief and misdemeanour

- Hermes supports default and temporary message types
  - Choice of which to leave at web interface
    - “I usually remember to stick up a post-it note only after locking the door behind me”*
  - Temporary messages can be
    - Cancelled by touching the screen
    - Selected from a user defined shortlist (e.g. ‘out to lunch’)
    - Increased use (83%→98% sharing context, but skewed content)
  - These operations are unauthenticated (in a hurry)
    - Could turn ‘out to lunch’ to ‘back tomorrow’
    - Yet seldom abused... even used positively... why?

# Social security

- Physicality of leaving messages
  - Visibility and ‘being caught in the act’ (night or right!)
  - Effort required to perpetrate (time, place)
  - Questionnaires reveal unwillingness to allow remote anonymous access
- Design for prevention
  - Unlike post-its, messages left to you are not public (c.f. graffiti)
  - Abuses are not very serious
  - Incentives are low
  - Misuse is unattractive

# Conclusion

- “Security is ensured, not by restricting access but by making activities visible”
  - Ever increasing number of public/ Ubicomp projects
  - Security for Ubicomp is a ‘grand challenge’
  - For certain classes of application
    - We have found that through careful design (incentive/ effort ratio)
    - And leverage on social behaviour (auditability)
    - Sufficient security can be achieved

<http://www.comp.lancs.ac.uk/~fittond/hermes/>