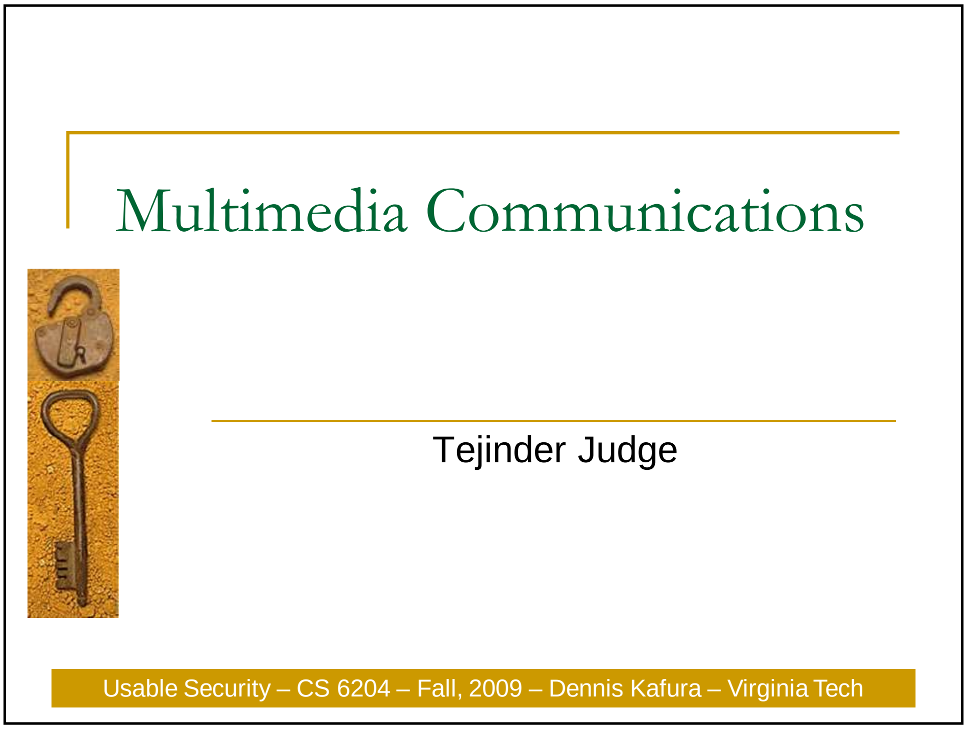
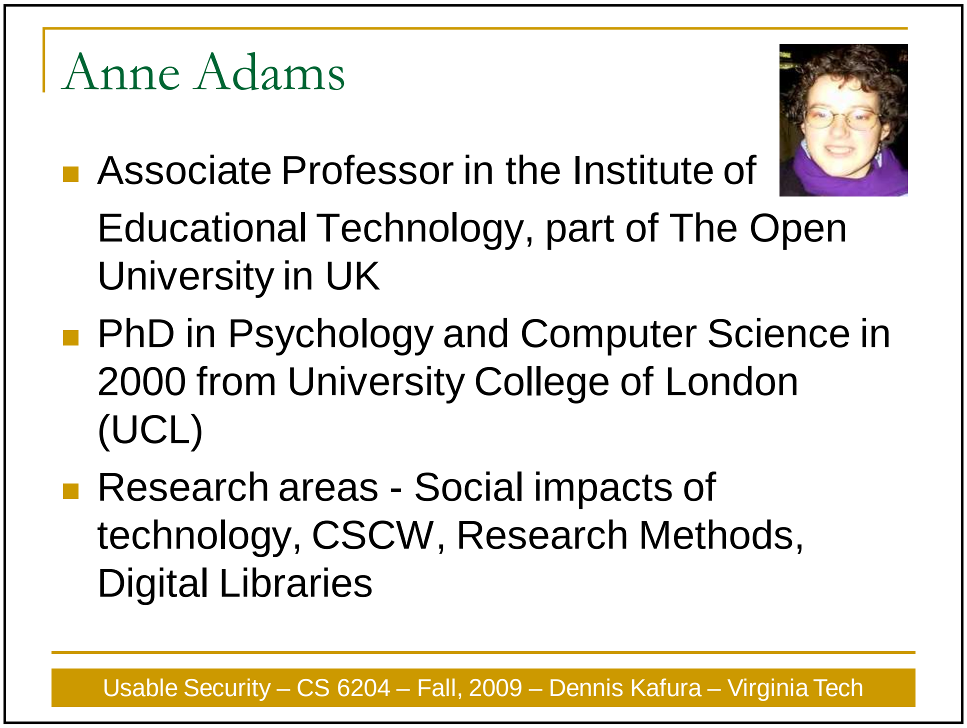


Multimedia Communications

Tejinder Judge



Anne Adams

- Associate Professor in the Institute of Educational Technology, part of The Open University in UK
- PhD in Psychology and Computer Science in 2000 from University College of London (UCL)
- Research areas - Social impacts of technology, CSCW, Research Methods, Digital Libraries

Central theme of these papers

- Perceived invasions of privacy can cause breakdowns in technologically mediated interactions, leading to user rejection of the technology
- Understanding users' perception of privacy will prevent resentment and rejection of multimedia systems

Paper 1

Users' perception of privacy in multimedia communication

Anne Adams

CHI '99 Extended Abstracts

Motivation

- Multimedia communication systems such as videoconferencing are becoming ubiquitous
- Accessing and using such systems increases privacy risks
- The aim of this research is to identify the mismatch between perceived and actual privacy risks

3 key privacy factors

- Information sensitivity
- Information receiver
- Information usage

Information sensitivity

- 2 levels of information
  - *Primary information* relates to the topic of discussion
  - *Secondary information* relays other characteristics about the user via visual, auditory or textural mediums
- When users discover data has a secondary level and it's being used in a way they did not anticipate, they feel that their privacy has been invaded

Information receiver

- Privacy can be invaded without users being aware of it
- Brings up the issue of whether it is *what is known* about a person that is invasive or *who knows it*

Information usage

- Users' fears of technology relate to the how their information is/will be used
- There is a relationship between the perceived information sensitivity and its potential receiver

Privacy model

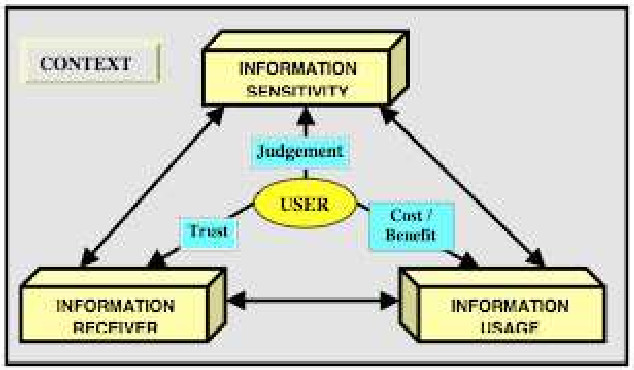
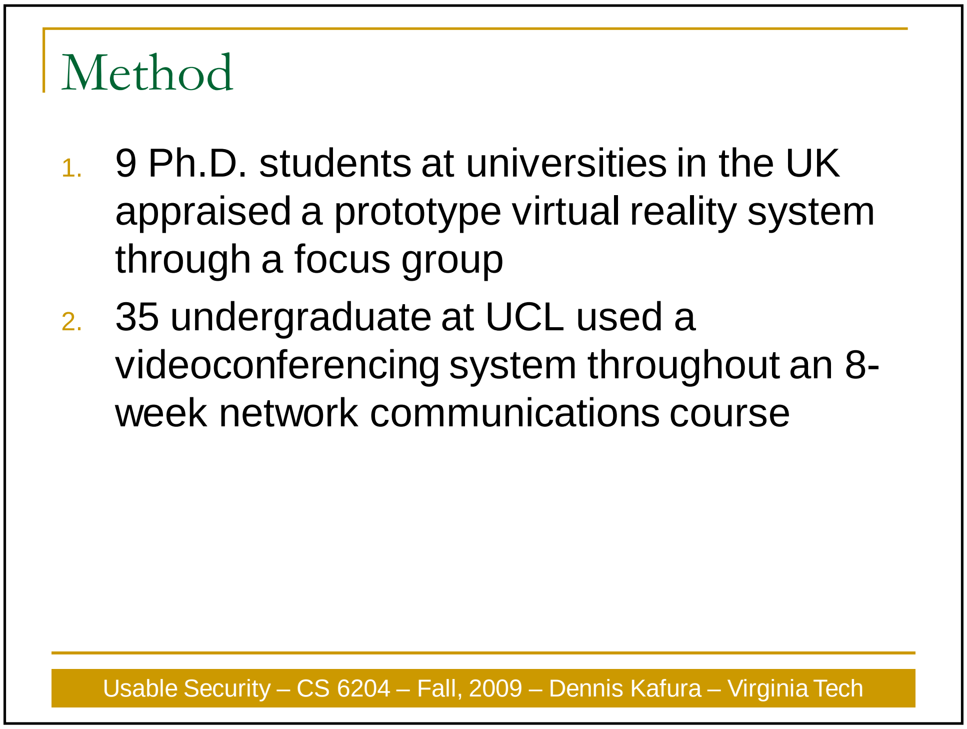
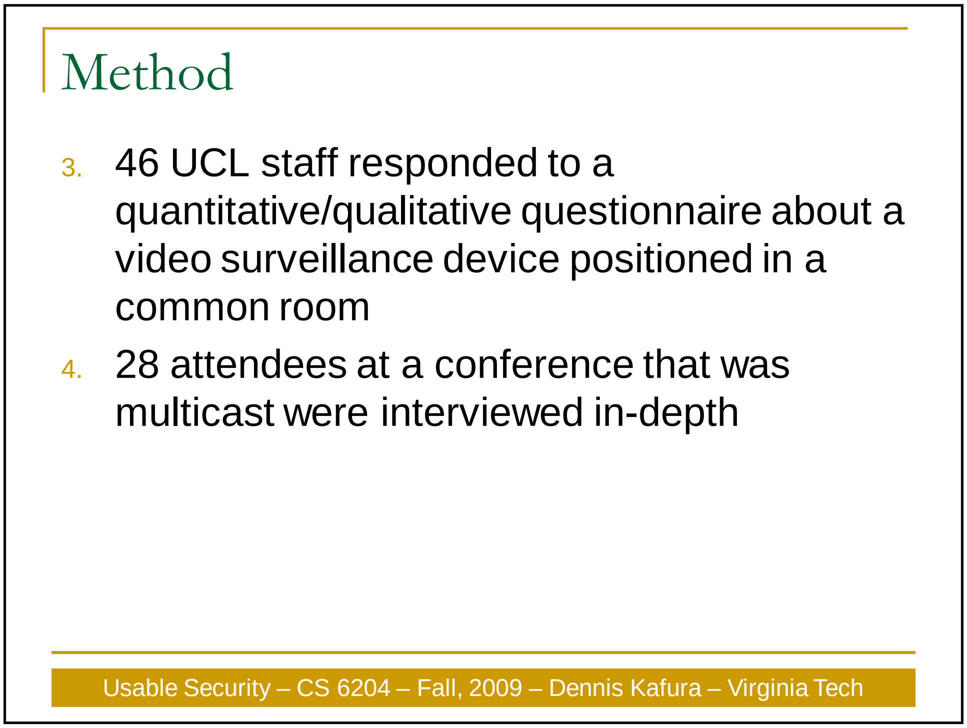


Figure 1: Privacy model factors and issues.



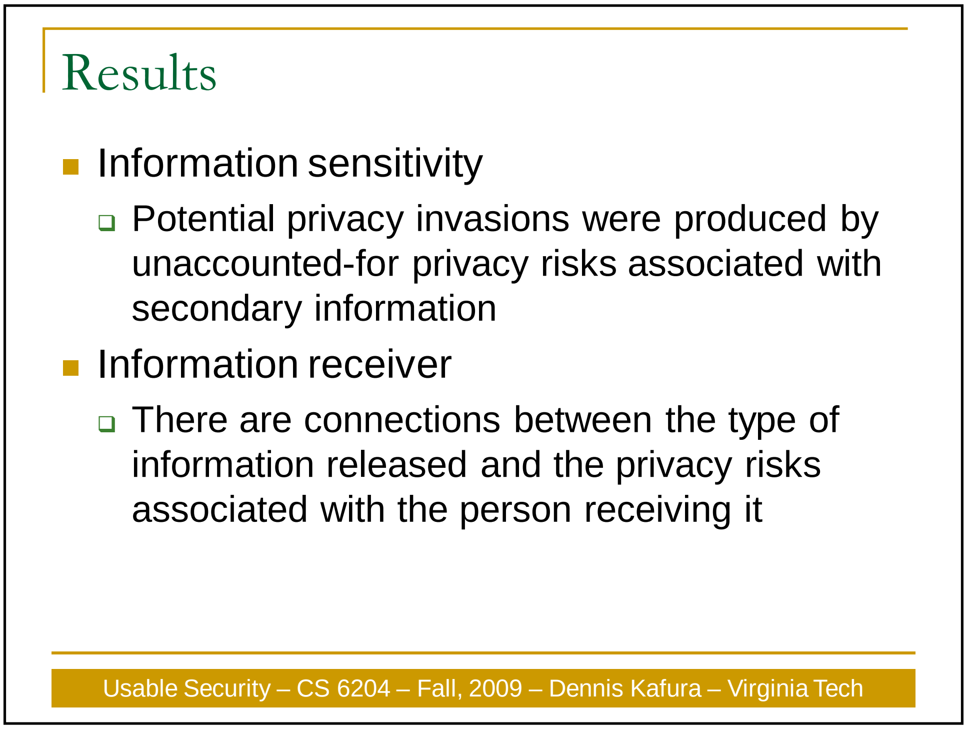
Method

1. 9 Ph.D. students at universities in the UK appraised a prototype virtual reality system through a focus group
2. 35 undergraduate at UCL used a videoconferencing system throughout an 8-week network communications course



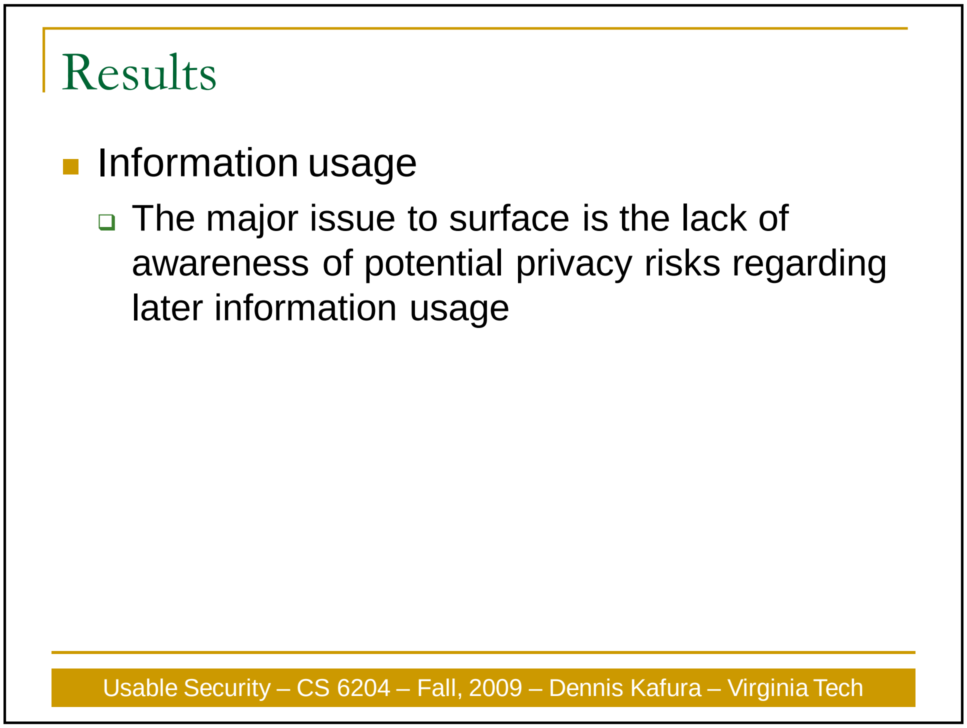
Method

3. 46 UCL staff responded to a quantitative/qualitative questionnaire about a video surveillance device positioned in a common room
4. 28 attendees at a conference that was multicast were interviewed in-depth



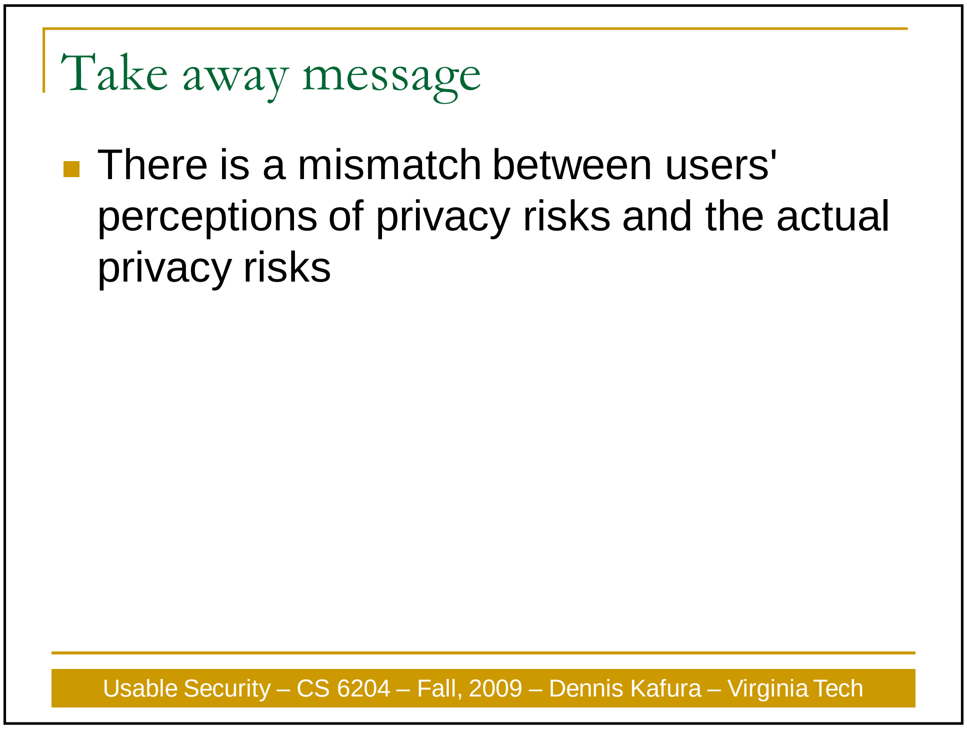
Results

- Information sensitivity
  - Potential privacy invasions were produced by unaccounted-for privacy risks associated with secondary information
- Information receiver
  - There are connections between the type of information released and the privacy risks associated with the person receiving it



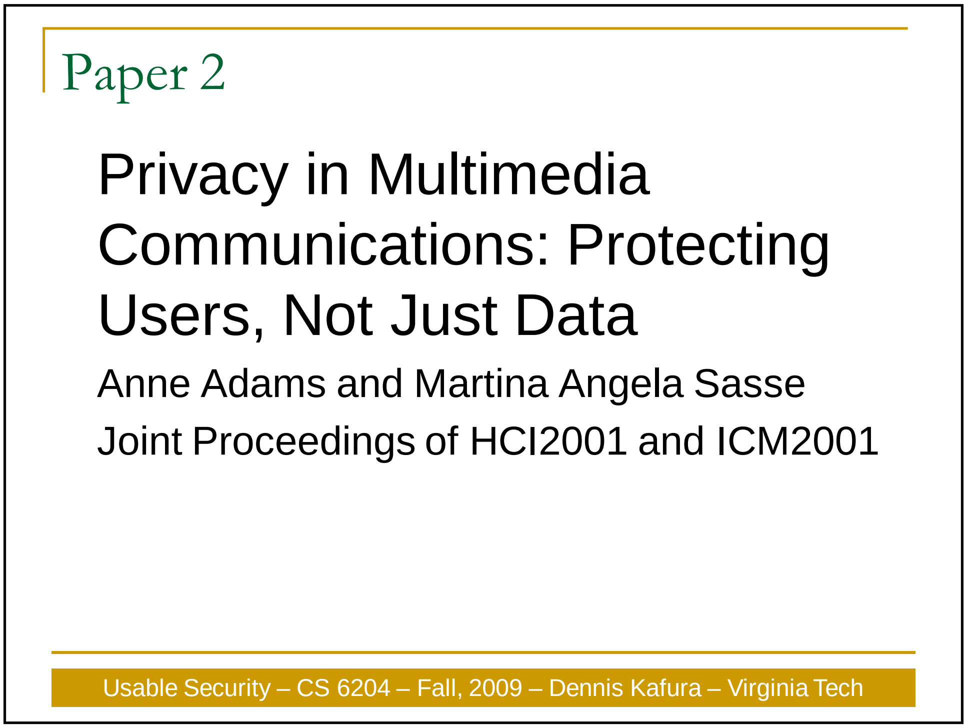
Results

- Information usage
  - The major issue to surface is the lack of awareness of potential privacy risks regarding later information usage



Take away message

- There is a mismatch between users' perceptions of privacy risks and the actual privacy risks

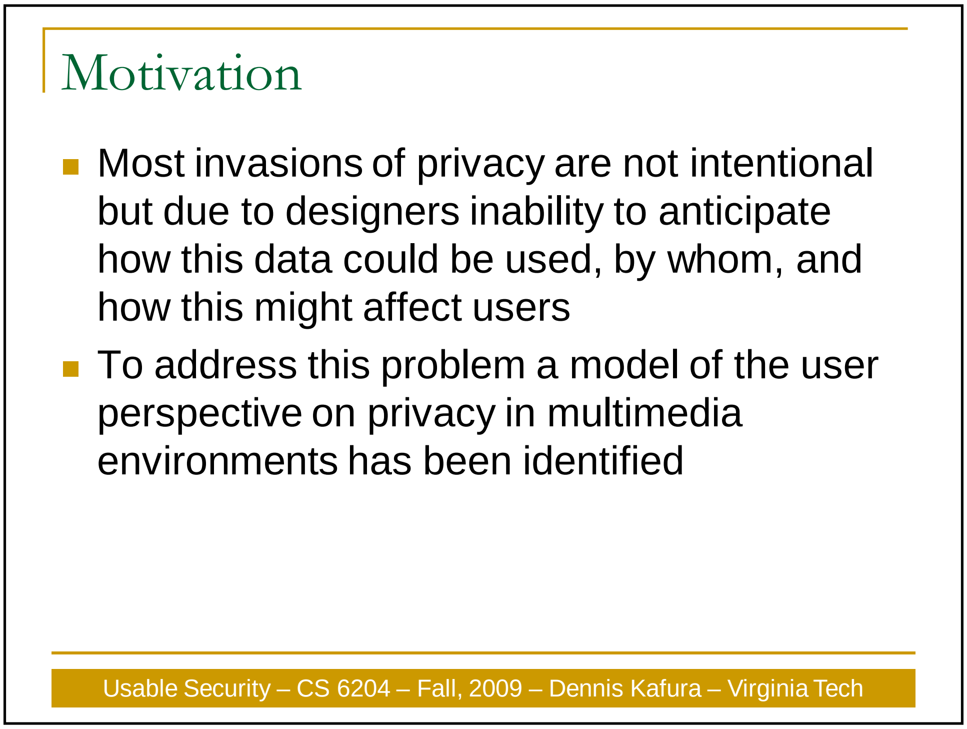


Paper 2

Privacy in Multimedia Communications: Protecting Users, Not Just Data

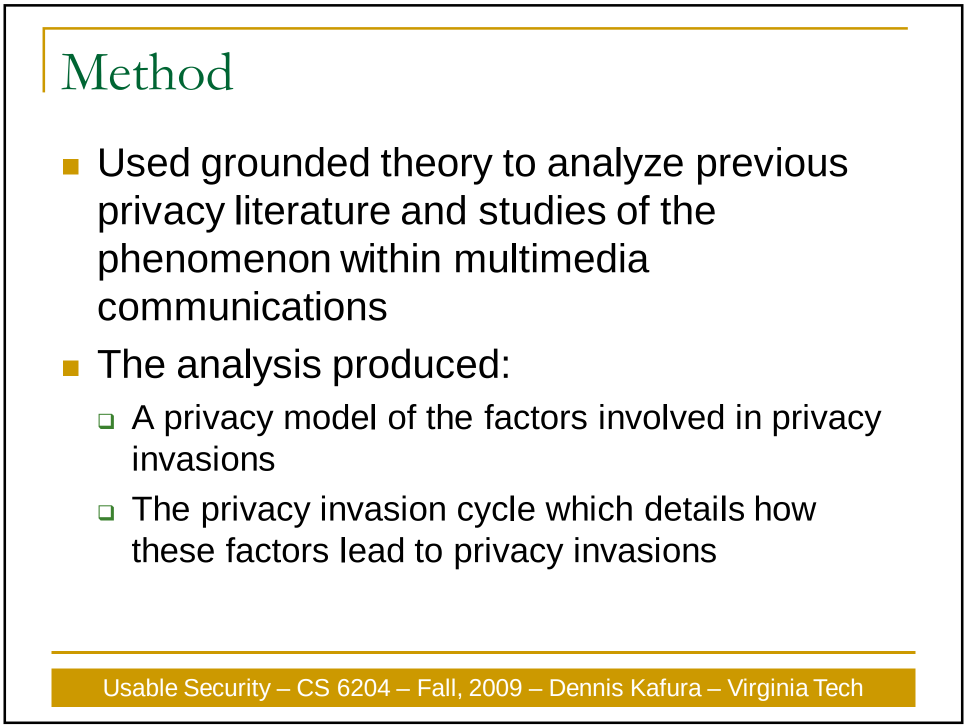
Anne Adams and Martina Angela Sasse

Joint Proceedings of HCI2001 and ICM2001



Motivation

- Most invasions of privacy are not intentional but due to designers inability to anticipate how this data could be used, by whom, and how this might affect users
- To address this problem a model of the user perspective on privacy in multimedia environments has been identified



Method

- Used grounded theory to analyze previous privacy literature and studies of the phenomenon within multimedia communications
- The analysis produced:
  - A privacy model of the factors involved in privacy invasions
  - The privacy invasion cycle which details how these factors lead to privacy invasions

Privacy model

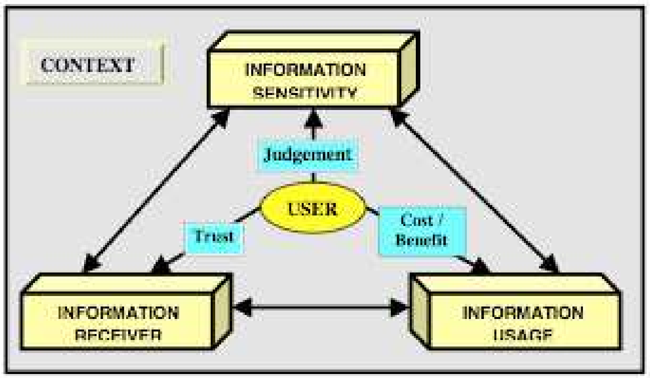


Figure 1: Privacy model factors and issues.

Privacy model - User

- Users are those who have data transmitted either directly (primary information or indirectly (secondary) about themselves
- Designers must understand that the user may well not be actively using the system and may actually be unaware that their data (their image, voice etc.) is being transmitted

Privacy model – Context

- Feedback of *what is being transmitted,* and control on *when information is being transmitted is required*
- Users need to have feedback about how they are being represented e.g. in videoconferencing
- What data is captured can affect how invasive the information is perceived to be

Privacy invasion cycle

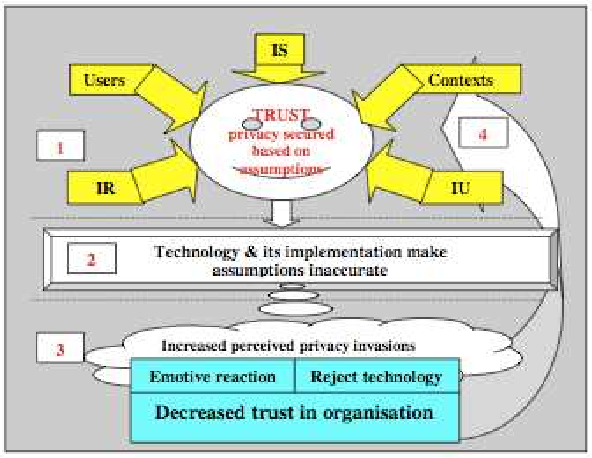
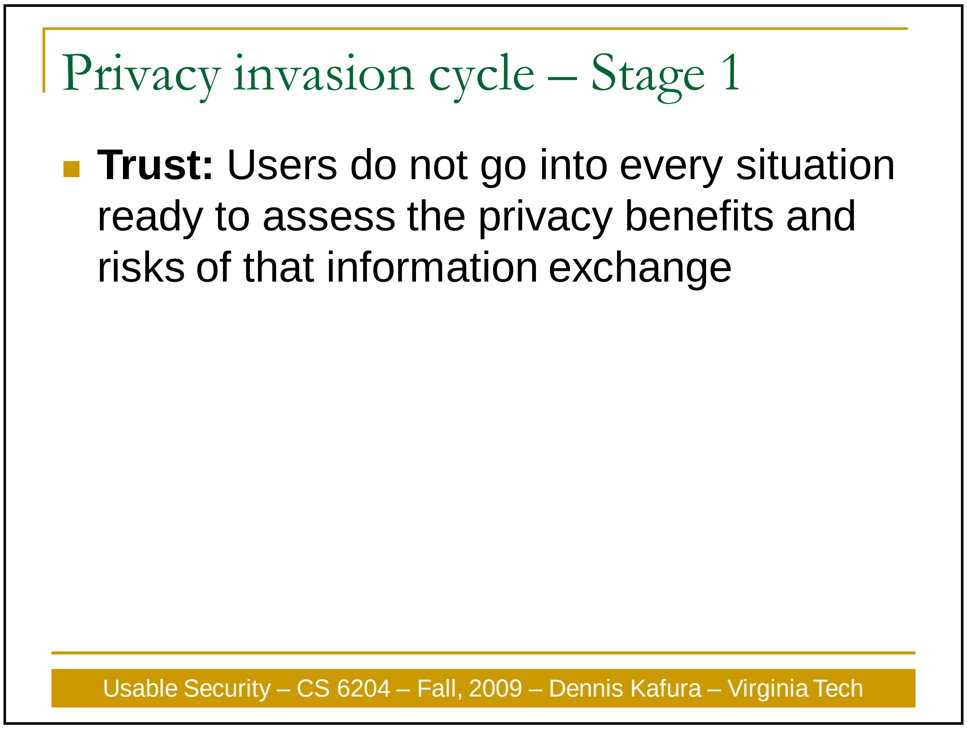

IS
Users
Contexts
TRUST
privacy secured
based on
assumptions
1
IR
IU
4
2
Technology & its implementation make assumptions inaccurate
3
Increased perceived privacy invasions
Emotive reaction
Reject technology
Decreased trust in organisation

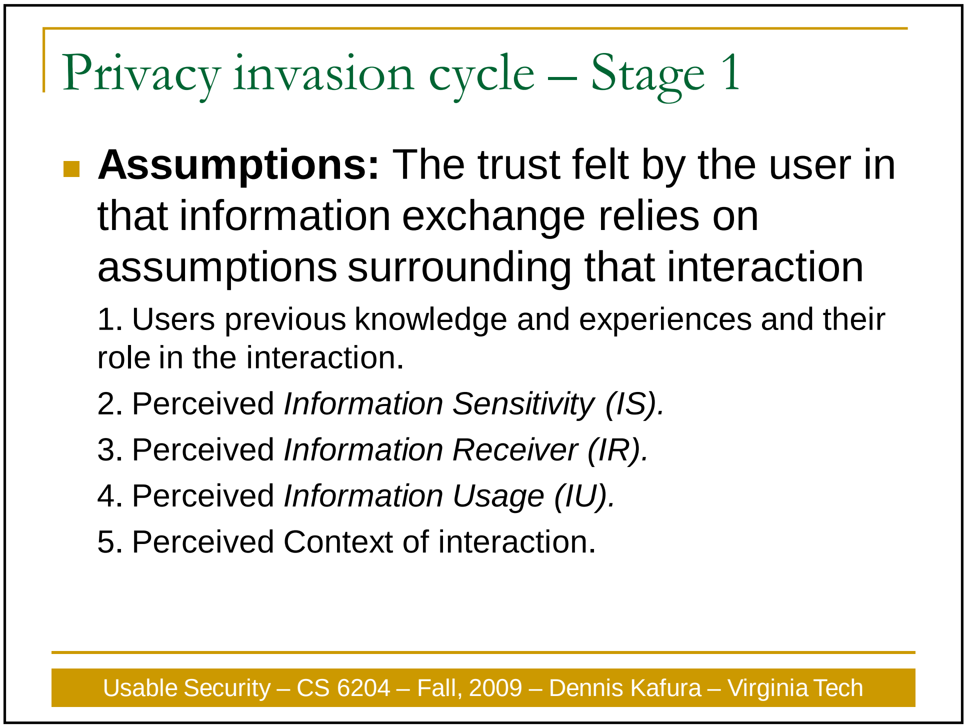
Figure 2: The privacy invasion cycle.



Privacy invasion cycle – Stage 1

- **Trust:** Users do not go into every situation ready to assess the privacy benefits and risks of that information exchange

Usable Security – CS 6204 – Fall, 2009 – Dennis Kafura – Virginia Tech



Privacy invasion cycle – Stage 1

- **Assumptions:** The trust felt by the user in that information exchange relies on assumptions surrounding that interaction

  1. Users previous knowledge and experiences and their role in the interaction.
  2. Perceived *Information Sensitivity (IS).*
  3. Perceived *Information Receiver (IR).*
  4. Perceived *Information Usage (IU).*
  5. Perceived Context of interaction.

Usable Security – CS 6204 – Fall, 2009 – Dennis Kafura – Virginia Tech

Privacy invasion cycle

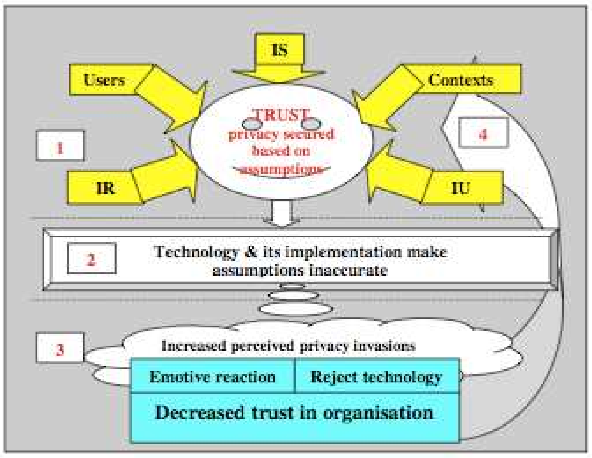


Figure 2: The privacy invasion cycle.

Privacy invasion cycle – Stage 3

- **Realization and Response:** When users realize that their assumptions were inaccurate, they experience an invasion of privacy

Privacy invasion cycle – Stage 4

- **Decreasing Cycle:** The next time the user encounters what they perceive to be a similar scenario their initial trust levels will be lowered

Privacy invasion cycle

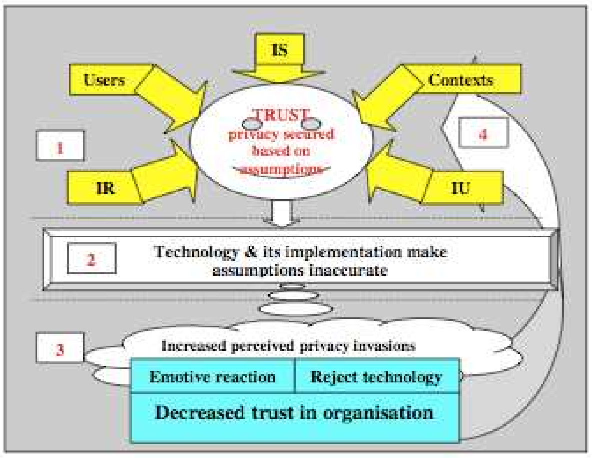


Figure 2: The privacy invasion cycle.

Privacy evaluation scenario

- Videoconferencing seminar was given from London to a local and remote (Glasgow) audience
- Both audiences had similar room setups
- Audience ranged from novices to experts in multimedia communication
  - Did not know remote audience or speaker
- All screens displayed 4 tiled windows
  - London audience, Glasgow audience, presenter, seminar slides/video

Privacy Recommendations

1. Briefing session
   - System details
   - Interaction details
   - Recording details

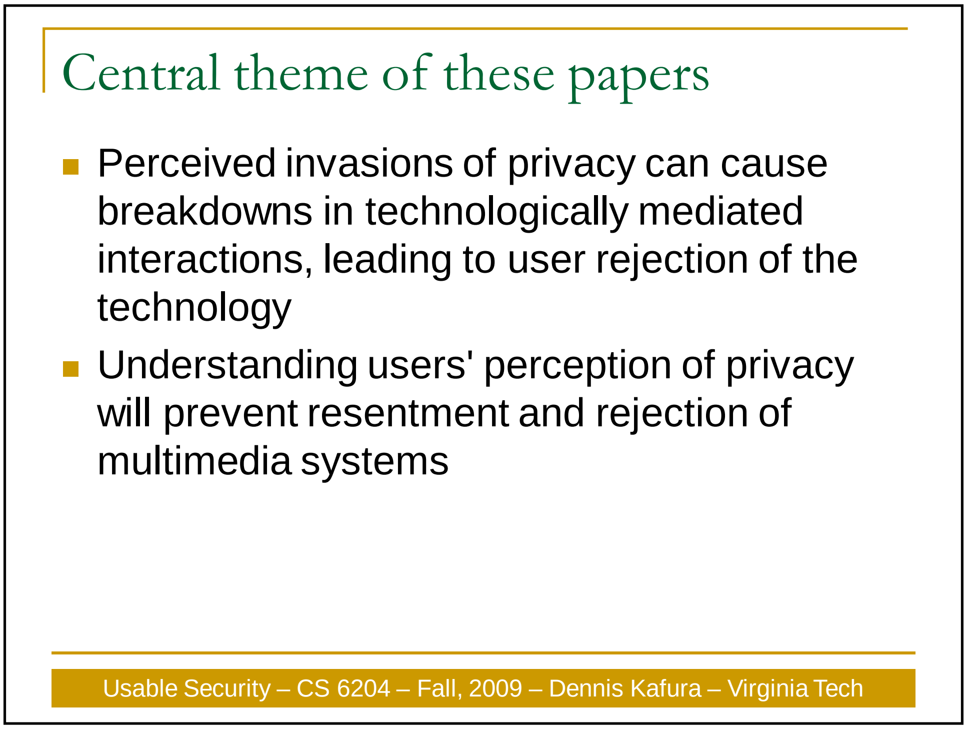
2. Information broadcaster
   - Data transmission
   - Interaction feedback
   - Recording feedback

Privacy recommendations

3. Information receiver
   - Contextual feedback
   - Edited data
   - Information handling
4. Policy procedures
   - Recording permission
   - Changed usage
   - Editing
   - Continued privacy evaluation

Take away message

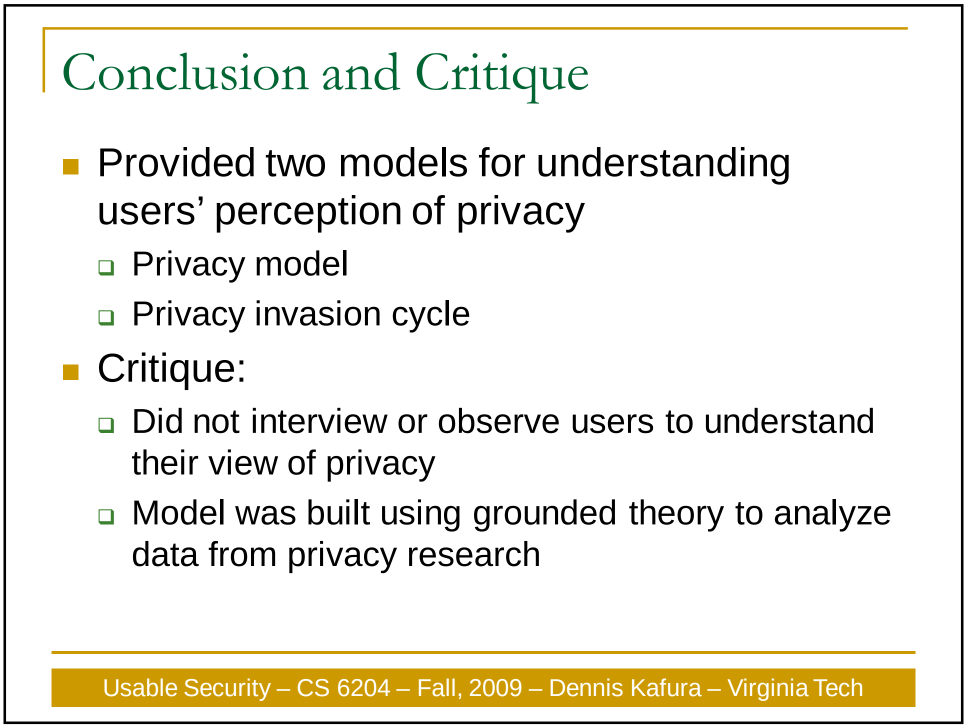
- These models detail what guides users' perceptions of privacy and provides a theory of the processes behind privacy invasions
- There is a need to counteract privacy problems before they arise thus solving them before people lose their trust and emotively reject the technology



Central theme of these papers

- Perceived invasions of privacy can cause breakdowns in technologically mediated interactions, leading to user rejection of the technology
- Understanding users' perception of privacy will prevent resentment and rejection of multimedia systems

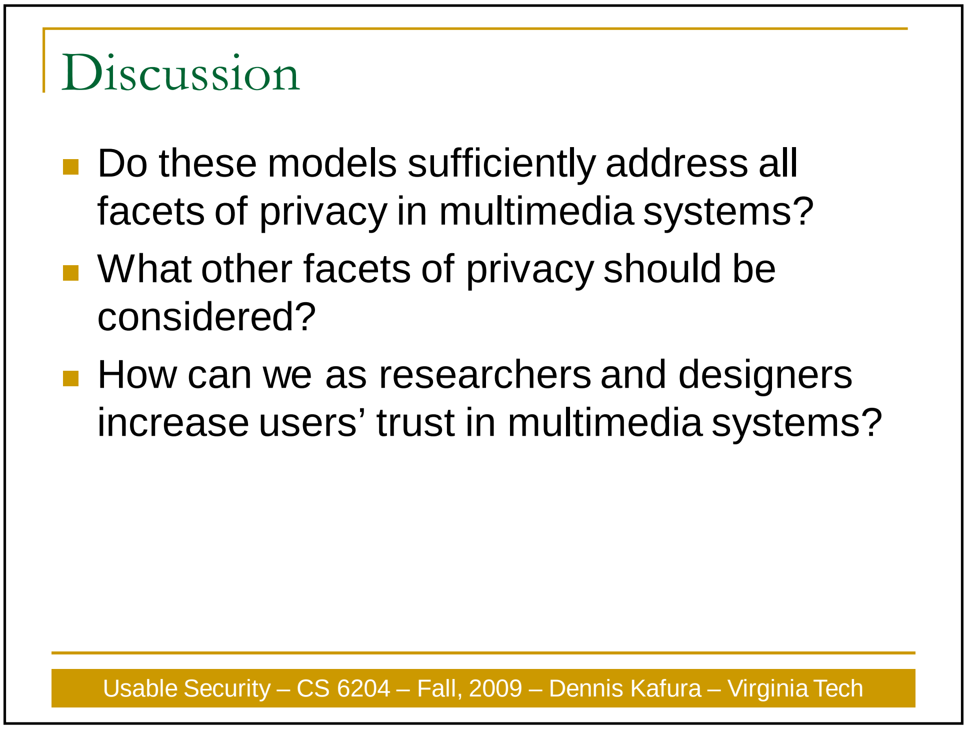
Usable Security – CS 6204 – Fall, 2009 – Dennis Kafura – Virginia Tech



Conclusion and Critique

- Provided two models for understanding users' perception of privacy
  - Privacy model
  - Privacy invasion cycle
- Critique:
  - Did not interview or observe users to understand their view of privacy
  - Model was built using grounded theory to analyze data from privacy research

Usable Security – CS 6204 – Fall, 2009 – Dennis Kafura – Virginia Tech



Discussion

- Do these models sufficiently address all facets of privacy in multimedia systems?
- What other facets of privacy should be considered?
- How can we as researchers and designers increase users’ trust in multimedia systems?