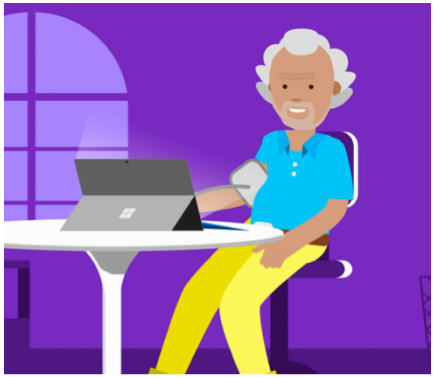
The Contextual Preferences of Older Adults on Information Sharing

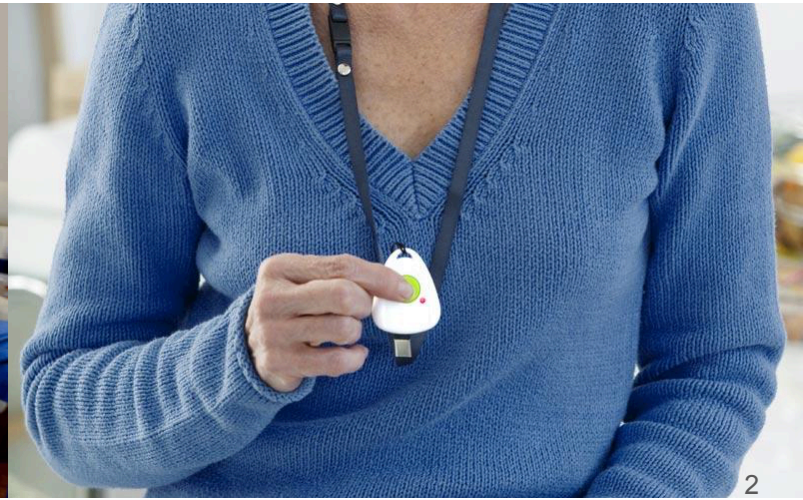


Alisa Frik,[1,2] Julia Bernd,[1] Florian Schaub,[3] Serge Egelman[1,2]

[1] International Computer Science Institute (ICSI), [2] University of California, Berkeley, [3] University of Michigan

ICSI Berkeley UNIVERSITY OF CALIFORNIA UNIVERSITY OF MICHIGAN NSF CLTC Center for Long-Term Cybersecurity UC Berkeley


6 PM
pillo



Motivation

The devices:

- Novel, innovative
- Complex
- Collect vast amounts of information
- Pose security and privacy risks

The older adults:

- Limited technical literacy and experience
- Declining physical and mental abilities
- Less aware and more susceptible to privacy and security risks

→ Research goal: Inform the design of effective systems that empower older adults to make informed decisions; to have better control over their personal data; and to maintain better security practices.

Method and Participants

- Semi-structured interviews (1.5 hours, $20)
- 46 participants from senior centers and senior residences in the San Francisco Bay Area
- Screened out those with cognitive impairments
- Ages 65-95 y.o. (mean=76)
- 64% live alone,
- 80% do not have a caregiver
- Female (65%)
- White (76%)
- Advanced (44%) or Bachelor’s (33%) degree

Interview Questions

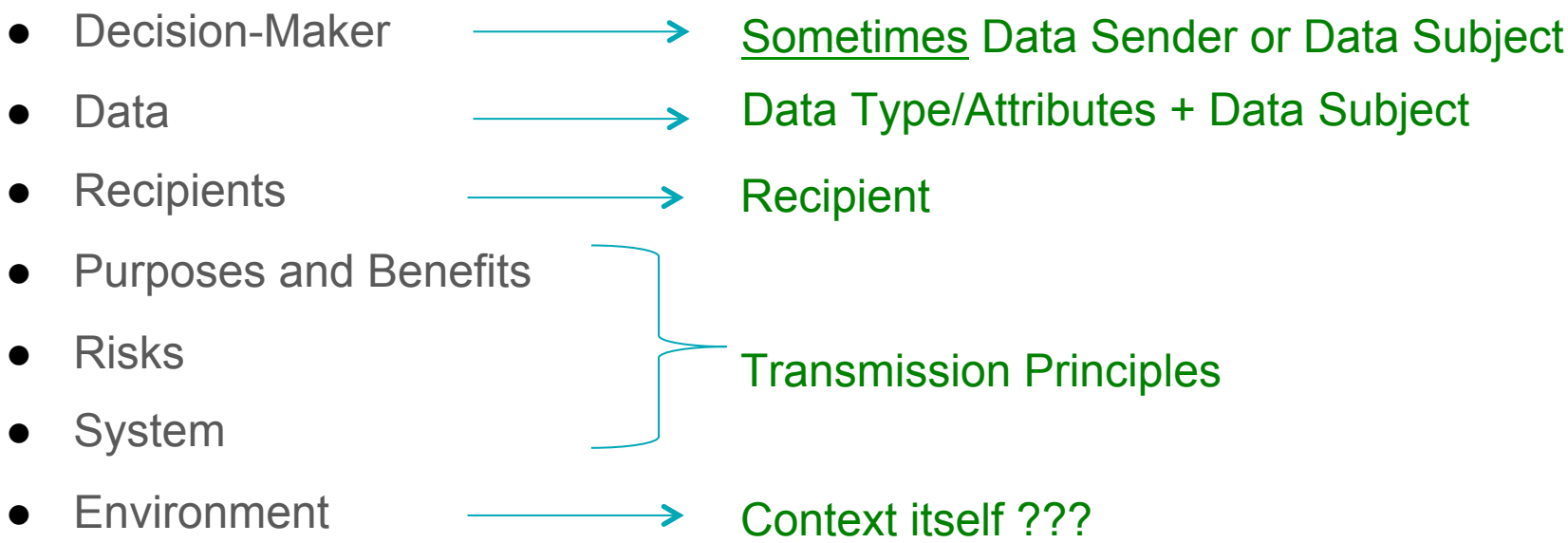
- What information
  - Do they expect to be collected, and what not?
  - Is ok to collect and share, and what not?
- With whom is ok to share, and with whom not?
- How it can be used and misused?

Dimensions

Based on thematic coding, we identified the following dimensions of information-sharing decision-making:

- Decision-Maker
- Data
- Recipients
- Purposes and Benefits
- Risks
- System
- Environment

Elements in our vs. CI framework



Aspects

- Decision-Maker
  - Privacy attitudes
  - Privacy expectations
  - Understanding of sharing scenarios
  - Technology acceptance
  - Degree of desire for agency/control
- Data
  - Relevance to recipient/goal
  - Requirement for data
  - Amount/extent
  - Accuracy, etc.

Factors

- Decision-Maker
  - Privacy attitudes
    - Personal experiences with violations
    - Risk attitudes
  - Privacy expectations
  - Understanding of sharing scenarios
    - Specific knowledge
    - Personal experience with a similar scenario
  - Technology acceptance
    - Technological self-efficacy
    - Need for sharing, etc.
  - Degree of desire for agency/control

Factors

- Decision-Maker
  - Privacy attitudes
    - Personal experiences with violations
    - Risk attitudes
  - Privacy expectations
  - Understanding of sharing scenarios
    - Specific knowledge
    - Personal experience with a similar scenario
  - Technology acceptance
    - Technological self-efficacy
    - Need for sharing, etc.
  - Degree of desire for agency/control

"Jews don't face the repression in this country today that we faced in my parent's generation, okay? [...] So I am never completely far removed from thoughts of political repression. [...] Nonetheless, I'm not ignorant of what's going on and what can go on. That's why I value privacy," P113

Data

- Data
  - Relevance to recipient/goal
  - Requirement for data (whether the data is necessary for fulfilling the goal)
  - Amount/extent
    - Volume
    - Breadth
    - Granularity
    - Format/sensor type
  - Accuracy, etc.
  - Data subject (self, others)

"The only thing [...] that I would be eager to share is the medical information, because anybody who has a right to know it, needs to know it. As to the other [types of information], it is really nobody else's business and I do take my privacy seriously. [...] I don't want to be bothered by people trying to sell me something," P113

Recipients

- Recipients
  - Trust in recipient
    - Evaluation of legitimacy
      - Past experiences with the relationship
      - Reputation
      - Assessment based on appearance/judgment
    - Evaluation of competence
  - Degree of removal from the initial act of data collection/sharing
  - Recipient’s potential reaction
    - Perceived desire to receive the data
    - Expected affective reaction
  - Humanness

Purposes and Benefits

- Purposes and Benefits
  - Domain of benefits
  - Who benefits accrue to
  - Perceived likelihood of benefit occurring
  - Extent of benefits
    - Importance or added value
    - Urgency / time sensitivity

Risks

- Risks

  Domain of potential risks

  - Perceived likelihood of the negative consequences happening
    - Related to the recipient’s purposes
    - Unrelated to the recipient’s purposes
  - Potential severity of consequences
  - Who accrues the consequences
  - Ability to protect against or mitigate the risks
    - Existence and availability of the mean of protection/mitigation
    - Cost of protection/mitigation (time and monetary)
    - Likely effectiveness

System

- System
  - Methods and policies
    - Data collection (including Continuance; and Interruption)
    - Data transmission (including Effort required to use the transmission channel; and Online vs. offline transmission channel)
    - Data storage (including Hosting; and Retention)
    - Data processing and use (including Human involvement)
  - Perceived security
    - On system/provider side
    - On user side

System (continued)

- System
  - Ability to control data flow
    - Which stages of the process can be controlled (including collection, further sharing, etc.)
    - Initiator of collection/sharing
    - Mechanism of control
    - Time and effort required to exert control
  - Transparency about data flows
    - Disclosure/notice (including channels, simplicity, specificity)
    - Ability to view/edit own data

Environment

- Environment
  - Sociocultural norms (including community, broader social, and legal)
    - Behavioral norms
    - Information-sharing norms
  - Stories
    - Media
    - Past experiences of close connections
  - Alternatives
    - Availability
    - Desirability (including convenience, effectiveness, cost, personalness)

Lessons Learned

- Paradigm examples are often *mentioned*,
  - but more granular preferences are *meant*
- Convergence of the parameters
- Contextual integrity framework can be expanded
- Other theories may plug in as well (Privacy Calculus, Protection Motivation Theory, etc.)

Future Work

- Validate the model
  - Against different populations and systems
  - Measure the relative importance of factors, and interactions
  - Revealed preferences (behavior) against stated preferences (attitudes/intentions)
- Turn the model into an actionable instrument (e.g. a deck of cards with the prompts for system designers)
- Map the intervention strategies against the model elements

Open questions to the audience:

- Does our model make sense to you?
- What are the other use cases for the model?

Alisa Frik: afrik@icsi.berkeley.edu