NC STATE UNIVERSITY

CSC 495.002 – Lecture 11
Usable Privacy: Decision Making and Warnings

Dr. Özgür Kafalı

North Carolina State University
Department of Computer Science

Fall 2017

NC STATE UNIVERSITY

AI for Privacy

- Privacy requirements
- Agents and reasoning
- Privacy norms
- Privacy breaches

What You Will Learn

- Human decision making
- Privacy engineering: Warnings and nudges
- Privacy policies and notices

Challenges in Privacy Decisions

- Benefits and costs associated with privacy decisions are complex
- Incomplete information, uncertainty
- Lack of knowledge about technological or legal forms of privacy protection
- A privacy concern is bundled with other useful functionality
- For example, a search query:
  - Get desired information
  - Give search engine information about user's interests
- Trade long term privacy for short term benefits

Acquisti and Grossklags. Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1):26–33, 2005

Privacy Attitudes

LEVEL OF CONCERN	GENERAL PRIVACY CONCERN (%)	DATA ABOUT OFFLINE IDENTITY (%)	DATA ABOUT ONLINE IDENTITY (%)	DATA ABOUT PERSONAL PROFILE (%)	DATA ABOUT PROFESSIONAL PROFILE (%)	DATA ABOUT SEXUAL AND POLITICAL IDENTITY(%)
High	53.7	39.6	25.2	0.9	11.9	12.1
Medium	35.5	48.3	41.2	16.8	50.8	25.8
Low	10.7	12.1	33.6	82.3	37.3	62.1

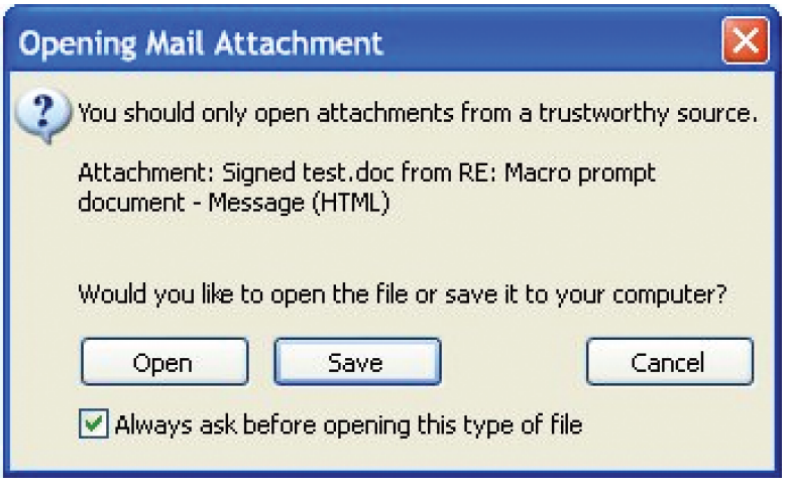
- Attitudes correlated with income
- More concerned with identifying information than profiling information
- 26% fundamentalists (high concern), 44% medium concern, 28% low concern

Bounded Rationality

- Even if complete information is available, hard to process such data
- Survey question: You completed a credit card purchase with an online merchant. Besides you and the merchant, who else has data about parts of your transaction?
- Nobody: 35%, bank 22%, hackers 19%
- When cued, participants would include those parties
- Participants considered a simplified mental model

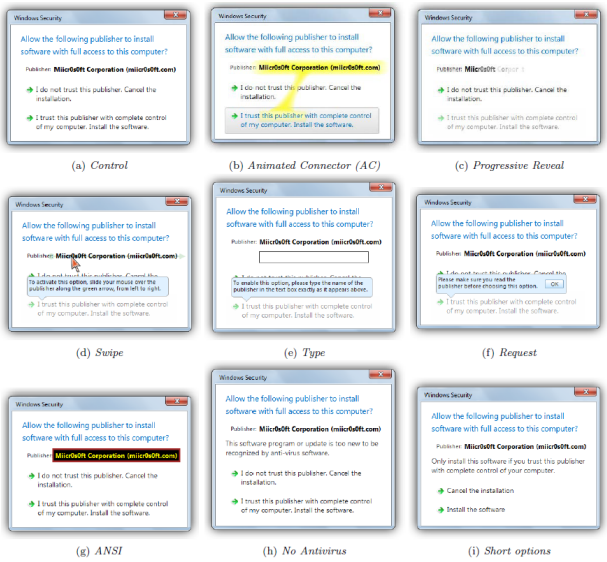
Simon. Models of Bounded Rationality. MIT Press, 1982

How Do Users Perceive Warnings?



Bravo-Lillo et al. Bridging the gap in computer security warnings: A mental model approach. IEEE Security and Privacy, 9(2):18–26, 2011

Warning Alternatives



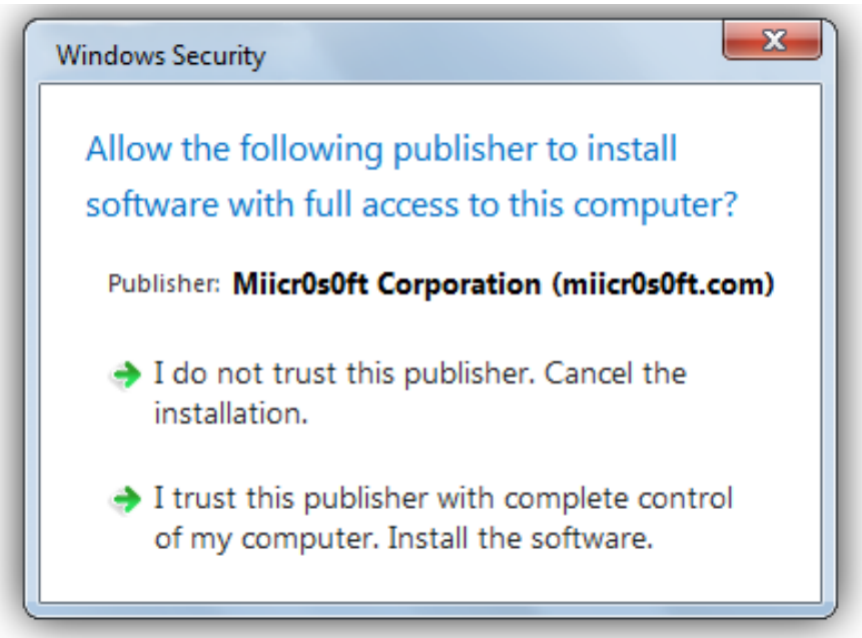
(a) *Control* (b) *Animated Connector (AC)* (c) *Progressive Reveal*

(d) *Swipe* (e) *Type* (f) *Request*

(g) *ANSI* (h) *No Antivirus* (i) *Short options*

Bravo-Lillo et al. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. Symposium on Usable Privacy and Security, 2013

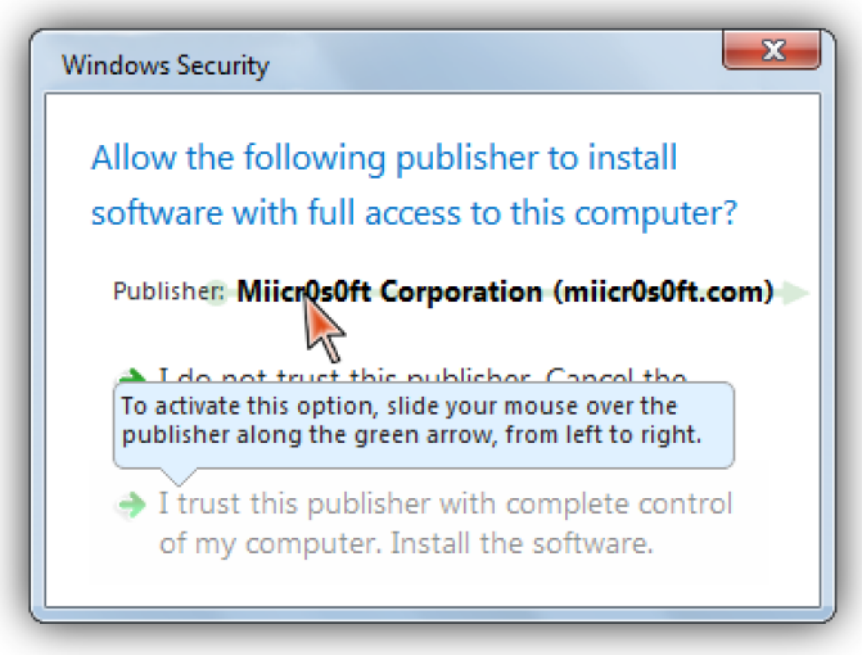
Control



Animated Connector

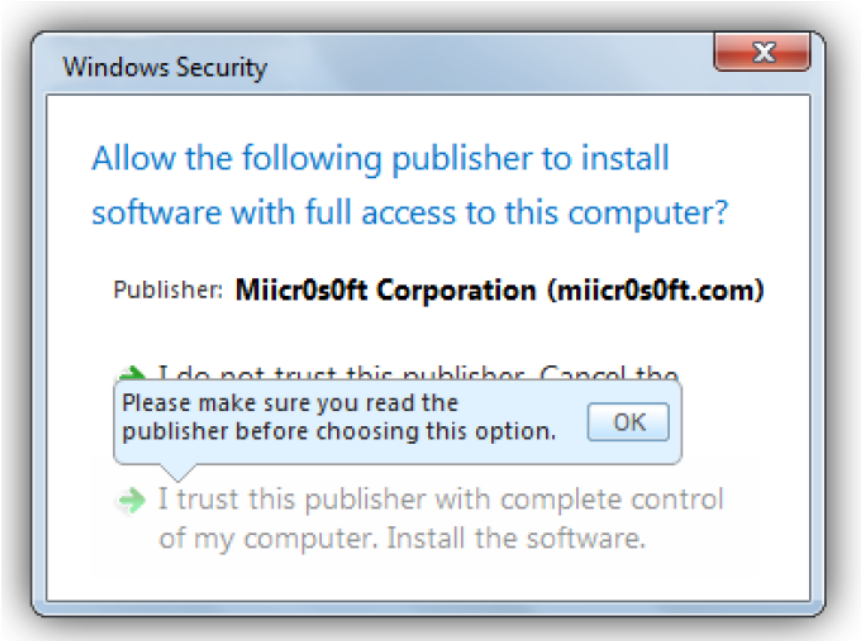
Progressive Reveal

Swipe



Type

Request



ANSI

No Antivirus

Short Options

Elevated Permissions

Pros/Cons

- Reduce the likelihood that participants
  - Install software from non legitimate publishers
  - Grant unnecessary permissions to apps
  - Fail to recognize instructions on a warning dialog
- Discourage users from performing useful actions (even when no risk is present)
- Delay typical workflows

Good Warning Design

- Determine the conditions before showing a warning
- Risks with unknown applications:
  - Might be malware
  - Access or misuse personally identifiable information
- A smart warning should eliminate the first alternative
- If free from malware, tailor the warning toward the second alternative

Advanced vs Novice Users

- Novice users assess an action after seeing its consequences
- Advanced users judge an action a priori
  - Look for vulnerabilities in public forums
  - Regularly patching software
  - Typing URLs directly rather than clicking a link

Novice Misconceptions

- Scenario where a bank's website produces an SSL warning:
- "I would hit yes, yes . . . I mean, assuming he trusts his bank. It's just, you know, the security certificate, you know, everything is valid about it, it's just you haven't elected to trust it yet, so I would feel better about hitting yes to that."
- Scenario about trusting a warning:
- "I guess the message looks authentic in terms of just the design, the icon used, and the font and the text and the gradient for the bar up top."

Exercise: Privacy Warning Design

- Revisit the meet up app for planning an activity: Assume it interacts with
  - Facebook to access similar users' profiles
  - Calendar to find out when users are free
  - Maps to find out where users spend time
  - Phone contacts to see call/text history
  - Weather app

- Design a usable privacy app: How would you
  - Detect suspicious/malicious activity by any of these apps?
  - Detect unusual actions/mistakes by novice users? And, warn them?
  - Make sure advanced users won't be annoyed by false alarms?

Privacy Nudges for Facebook

A Field Trial of Privacy Nudges for Facebook

Yang Wang,[‡] Pedro Giovanni Leon,[*] Alessandro Acquisti,[*]
Lorrie Faith Cranor,[*] Alain Forget,[*] and Norman Sadeh[*]

[‡]Syracuse University
ywang@syr.edu

[*]Carnegie Mellon University
{pedrogln, acquisti, lorrie, aforget, sadeh}@cmu.edu

ABSTRACT

Anecdotal evidence and scholarly research have shown that Internet users may regret some of their online disclosures. To help individuals avoid such regrets, we designed two modifications to the Facebook web interface that nudge users to consider the content and audience of their online disclosures more carefully. We implemented and evaluated these two nudges in a 6-week field trial with 28 Facebook users. We analyzed participants' interactions with the nudges, the content of their posts, and opinions collected through surveys. We found that reminders about the audience of posts can prevent unintended disclosures without major burden; however, introducing a time delay before publishing users' posts can be perceived as both beneficial and annoying. On balance, some participants found the nudges helpful while others found them unnecessary or overly intrusive. We discuss implications and challenges for designing and evaluating systems to assist users with online disclosures.

making. These biases are systematic deviations from what traditional economists call rational decisions. Furthermore, when limited resources (e.g., time or information) are available to make a decision, human beings often rely on heuristics or shortcuts. These biases and heuristics have been shown to impact privacy decisions [1, 4, 5] and privacy blunders in social media are vivid examples of the hurdles users face.

Behavioral economists have proposed the use of soft paternalistic interventions to help people overcome behavioral biases that affect decision making. These interventions are designed to "nudge" (instead of force) people towards behaviors that have been shown to be publicly desired, but difficult to follow, without limiting people's autonomy [24]. Acquisti has proposed to use soft paternalistic interventions to improve security and privacy decisions [2]. We refer to soft-paternalistic mechanisms that nudge people towards more thoughtful and informed privacy-related decisions as *privacy nudges*.

Wang et al. A Field Trial of Privacy Nudges for Facebook. Conference on Human Factors in Computing Systems, pages 2367–2376, 2014

Objectives

- Help users better understand the audience for their posts
- Users underestimate their audience: 27% of its true size
- Context collapse: Communicate with many groups simultaneously
- Interventions to “nudge” users (soft paternalistic mechanisms)
- Preserve autonomy: Not force users to do so

Nudges

- Multidisciplinary research to assist users with privacy decision making
  - Human computer interaction
  - Persuasive technology
- Create stronger passwords: Password strength meter
- Mobile app selection
- Facebook interface changes

Nudge Design

- Design based on lessons learned from pilot studies
- Audience nudge: Remind users about the audience for their post
- Timer nudge: Make users pause and think before posting

Audience Nudge

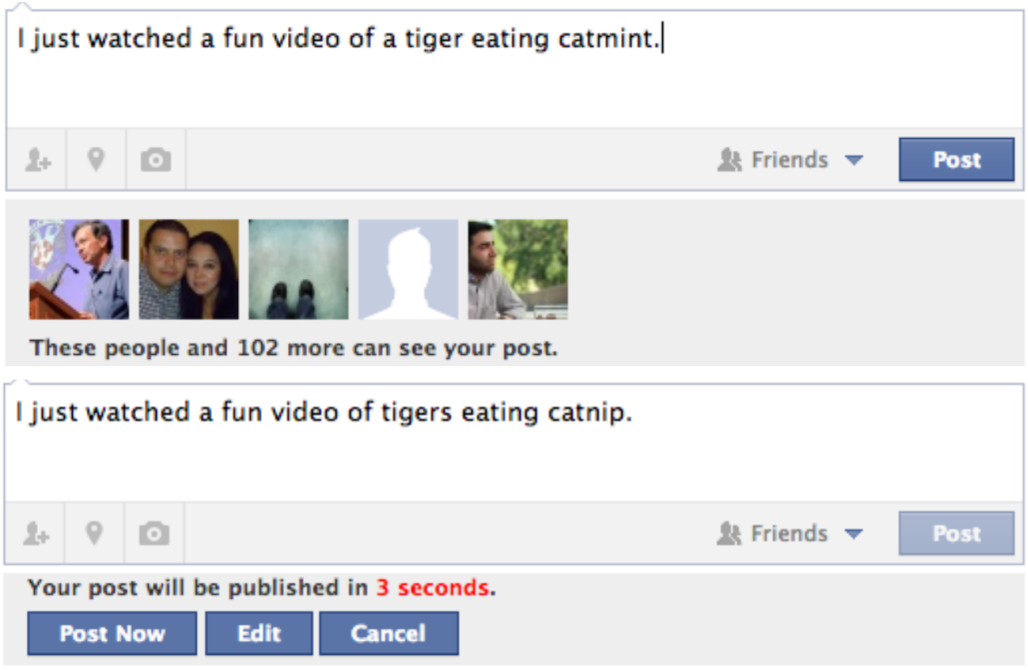
- Inspired by “bounded rationality”
- Intervention message: These [number] of people can see this post
- Show visual rather than textual cues
- Show profile pictures of five random people who can see the post
- “Identifiable victim effect”
- New message: These people and [number] more can see your post

Timer Nudge

- Inspired by “hyperbolic time discounting”
- People would be indifferent between receiving $15 immediately or $30 after 3 months, $60 after 1 year, or $100 after 3 years

- Initial version: 20 second delay between user clicking post and actual publishing
- During the countdown, user can cancel the post
- Reduced time delay to 10 seconds
- User can: Post now, edit, or cancel
- Facebook look and feel for the buttons

Audience and Timer Nudges



Interactions with Nudges

- Four common behavior patterns among 28 participants
- Hover over profile pictures: 24 checked out pictures at least three times
- Click “Post Now”:
  - 24 clicked for status updates, 26 clicked for comments at least once
  - More often for status updates (64%) than comments (25%)
- Click “Edit”: Five clicked for status updates, 18 clicked for comments
- Click “Cancel”: Less than 1% of all posts

Participant Categories

- Participants grouped into five categories
- Frequent interactions and positive attitude: 4
- Limited interactions and positive attitude: 10
- Limited interactions and negative attitude: 3
- Frequent interactions and negative attitude: 7
- Indifferent: 4

Limitations and Implications

- Hawthorn effect: Participants may change behavior simply because they're in a study
- Intrusiveness of nudges: Less intrusive "audience" nudge better received than "timer" nudge
- Function properly: Do not interfere with usability or break functionality

Broadcasting Location History

- News article: https://www.eff.org/deeplinks/2014/07/your-android-device-telling-world-where-youve-been
- Links are also on the course website

Things to Look For

- Root cause: What went wrong?
- If it was not intentional, what was the original aim?
- Affected parties
- Implications and similar problems
- Mitigation (using methods we have seen): Prevention, detection, recovery

- Take 10 minutes to look at the incident on your own

- Now discuss with your neighbor
- Also take a look at the summary report: https://drive.google.com/file/d/0B3m-I0YVAv0ELTRLeVpTWlZaQlU/view