Privacy in the Age of Augmented Reality

Alessandro Acquisti

Carnegie Mellon University

USENIX 2011

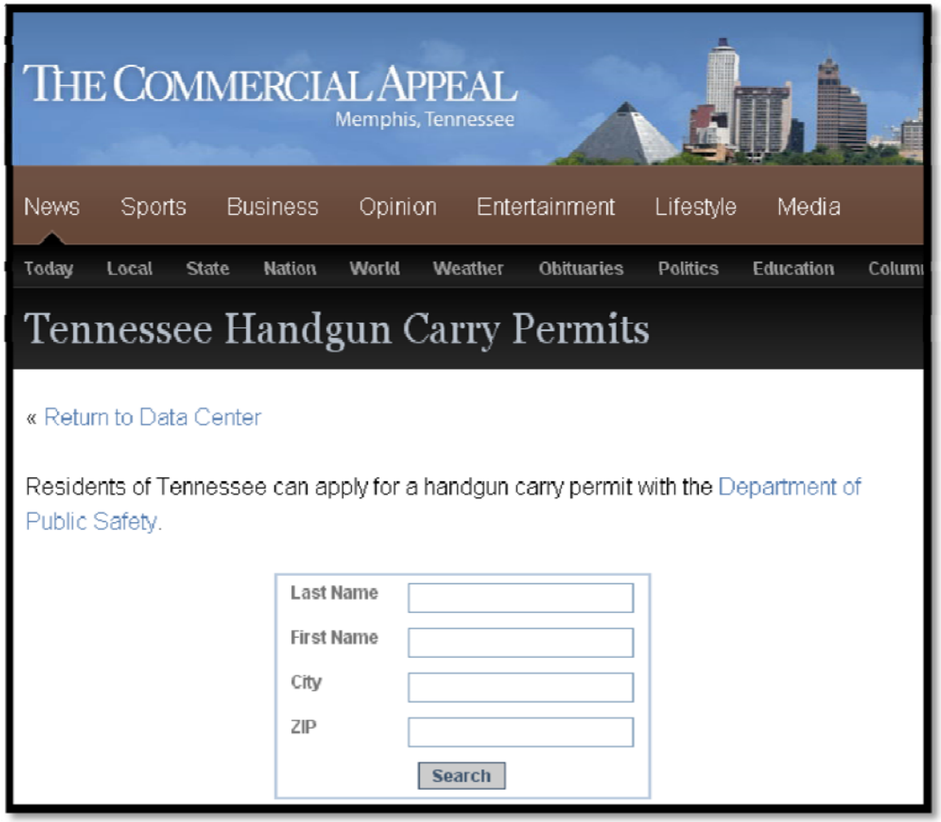
[redacted]

- *What are the trade-offs associated with protecting and sharing personal information?*
- *How rationally do we calculate, and make decisions about, those trade-offs?*
- *What are the consequences of those decisions?*
- *How will new technologies influence those decisions, and their consequences?*

Background

- From the economics of privacy…
  - *Protection and revelation of personal data flows involve* ***tangible and intangible*** *trade-offs for the* ***data subject*** *as well as the potential* ***data holder***

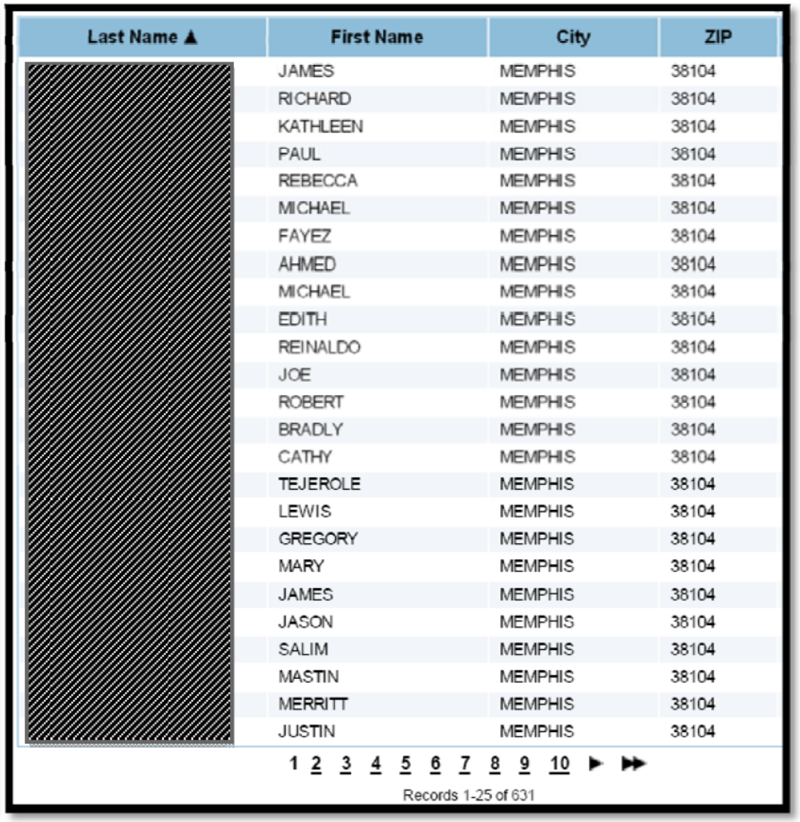
Guns, privacy, and crime



Tennessee Handgun Carry Permits

« Return to Data Center

Residents of Tennessee can apply for a handgun carry permit with the Department of Public Safety.



Last Name ▲	First Name	City	ZIP
[redacted]	JAMES	MEMPHIS	38104
[redacted]	RICHARD	MEMPHIS	38104
[redacted]	KATHLEEN	MEMPHIS	38104
[redacted]	PAUL	MEMPHIS	38104
[redacted]	REBECCA	MEMPHIS	38104
[redacted]	MICHAEL	MEMPHIS	38104
[redacted]	FAYEZ	MEMPHIS	38104
[redacted]	AHMED	MEMPHIS	38104
[redacted]	MICHAEL	MEMPHIS	38104
[redacted]	EDITH	MEMPHIS	38104
[redacted]	REINALDO	MEMPHIS	38104
[redacted]	JOE	MEMPHIS	38104
[redacted]	ROBERT	MEMPHIS	38104
[redacted]	BRADLY	MEMPHIS	38104
[redacted]	CATHY	MEMPHIS	38104
[redacted]	TEJEROLE	MEMPHIS	38104
[redacted]	LEWIS	MEMPHIS	38104
[redacted]	GREGORY	MEMPHIS	38104
[redacted]	MARY	MEMPHIS	38104
[redacted]	JAMES	MEMPHIS	38104
[redacted]	JASON	MEMPHIS	38104
[redacted]	SALIM	MEMPHIS	38104
[redacted]	MASTIN	MEMPHIS	38104
[redacted]	MERRITT	MEMPHIS	38104
[redacted]	JUSTIN	MEMPHIS	38104

Records 1-25 of 631

Background

- From the economics of privacy…
  - *Protection and revelation of personal data flows involve* ***tangible and intangible*** *trade-offs for the* ***data subject*** *as well as the potential* ***data holder***

- … to the behavioral economics of privacy
  - Incomplete information
  - Bounded rationality
  - Cognitive/behavioral biases

- … to online social networks

Background

- From the economics of privacy…
  - *Protection and revelation of personal data flows involve **tangible and intangible** trade-offs for the **data subject** as well as the potential **data holder***

- … to the behavioral economics of privacy
  - Incomplete information
  - Bounded rationality
  - Cognitive/behavioral biases

- … to online social networks and data mining

Today

- I will try and connect two streams of my research
  1. Three studies about the **challenges we face when making decisions about our privacy**
  2. One study about the **privacy issues arising from the convergence of various technologies** (online social networks, face recognition, and cloud computing)

Four studies

1. The inconsistency of privacy valuations
2. The paradox of control
3. Discounting past information
4. Faces of Facebook: Privacy and face recognition

Four studies

1. **The inconsistency of privacy valuations**
   - **With Leslie John and George Loewenstein**
2. The paradox of control
3. Discounting past information
4. Faces of Facebook: Privacy and face recognition

The inconsistency of privacy valuations

- Can mere framing change the valuation of personal data?

  Consider:

  - Willingness to accept (WTA) money to give away information

    vs.

  - Willingness to pay (WTP) money to protect information
- Hypothesis:
  - People assign different values to their personal information depending on whether they are focusing on **protecting it** or **revealing it**
    - Related to the endowment effect (e.g., Thaler 1980)

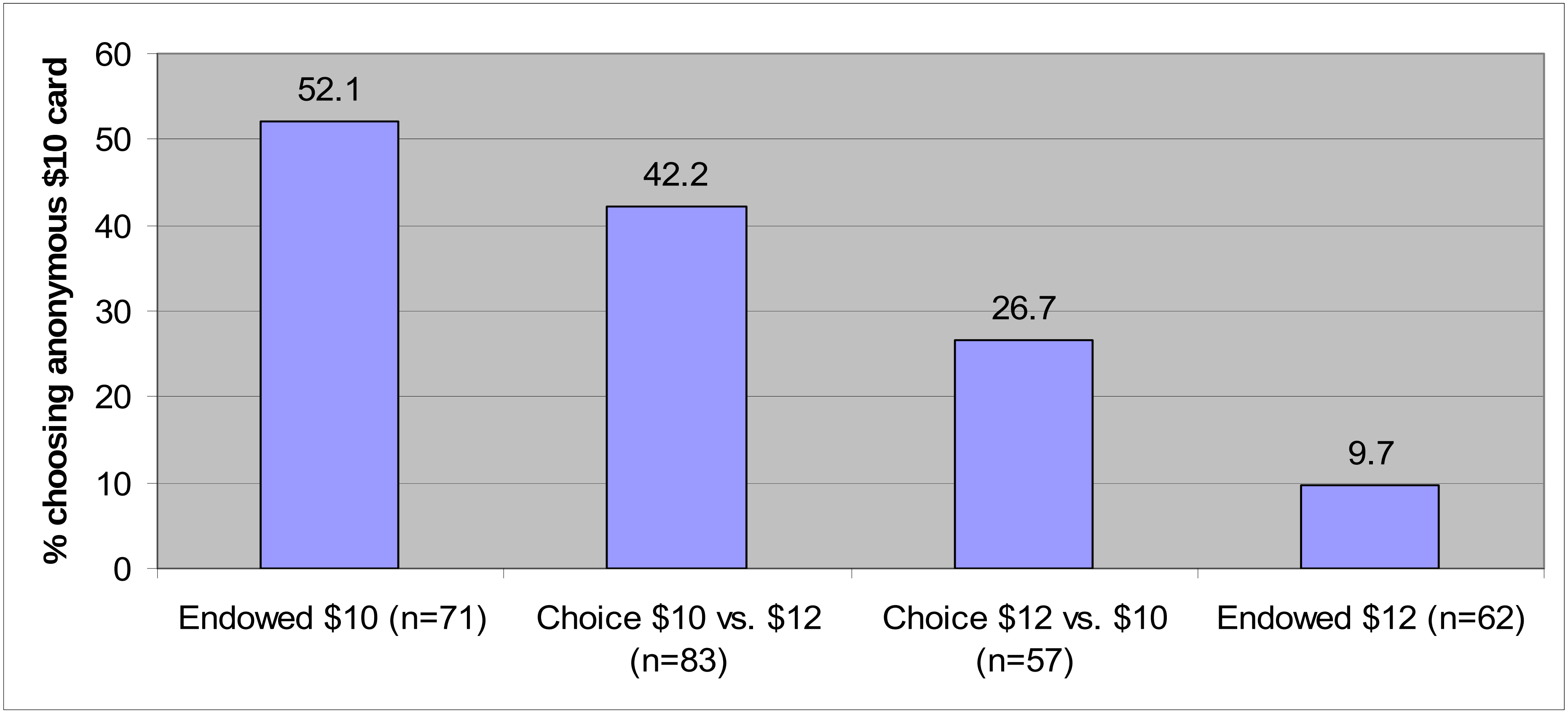
Experimental design

- Mall patrons asked to participate in (decoy) survey
- As payment for participation, subjects were offered gift cards
- We manipulated trade-offs between privacy protection and value of cards

Experimental design

- Subjects *endowed* with either:
  - **$10 Anonymous gift card.** "*Your name will not be linked to the transactions completed with the card, and its usage will not be tracked by the researchers.*"
  - **$12 Trackable gift card.** "*Your name will be linked to the transactions completed with the card, and its usage will be tracked by the researchers.*"
- Subjects asked whether they'd like to *switch* cards
  - From $10 Anonymous to $12 Trackable (WTA)
  - From $12 Trackable to $10 Anonymous (WTP)

WTP vs. WTA: Results



Implications

- People’s concerns for privacy (and security) depend, in part, on priming and framing
- Vicious circle: if you have *less privacy*, *you value privacy less*

Four studies

1. The inconsistency of privacy valuations
2. **The paradox of control**
   - **With Laura Brandimarte and George Loewenstein**
3. Discounting past information
4. Faces of Facebook: Privacy and face recognition

Privacy and the paradox of control

Control :: Privacy

+

Privacy and the paradox of control

Control :: Privacy

=

Privacy and the paradox of control

Control :: Privacy

-

Conjecture

- When deciding what to reveal about ourselves, we may confound
  1. control over **publication** of private information, and
  2. control over **access/use** of that information by others
- … and end up giving more weight to the former over the latter
  - Even though **objective privacy costs derive from access to/use** of information by others, not merely its publication
- Why?
  - Saliency (Slovic, 1975; Klein, 1998) of act of publishing
  - Overconfidence
  - See also Henslin 1967, Langer 1975

Two hypotheses

- *Subjects induced to perceive* ***more control over publication*** *of personal information, even though in reality they* ***face the same (or even higher) objective risks associated with the access and use*** *of that information,* ***will disclose more sensitive information and/or more widely***

- *Users induced to perceive* ***less control over publication*** *of personal information, even though in reality they do* ***not face higher objective risks*** *associated with the access and use of that information,* ***will disclose less sensitive information and/or less widely***

Three survey-based randomized experiments

- We ran three survey-based randomized experiments
- In some of them we **reduced** perceived control over publication of personal information
- In some of them we **increased** perceived control over publication of personal information
  - E.g., Experiment 3

Experiment 3

- Design
  - Subjects: 100+ CMU students recruited on campus, March 2010
  - Completed online survey
  - Justification for the survey: study on ethical behaviors
  - Ten Yes/No questions that focused on sensitive behaviors (e.g. drug use, stealing)
    - Included demographics + privacy intrusive and non-intrusive questions (as rated by 49 subjects independently in a pre-study)
  - DV: Answer/No answer

Experiment 3

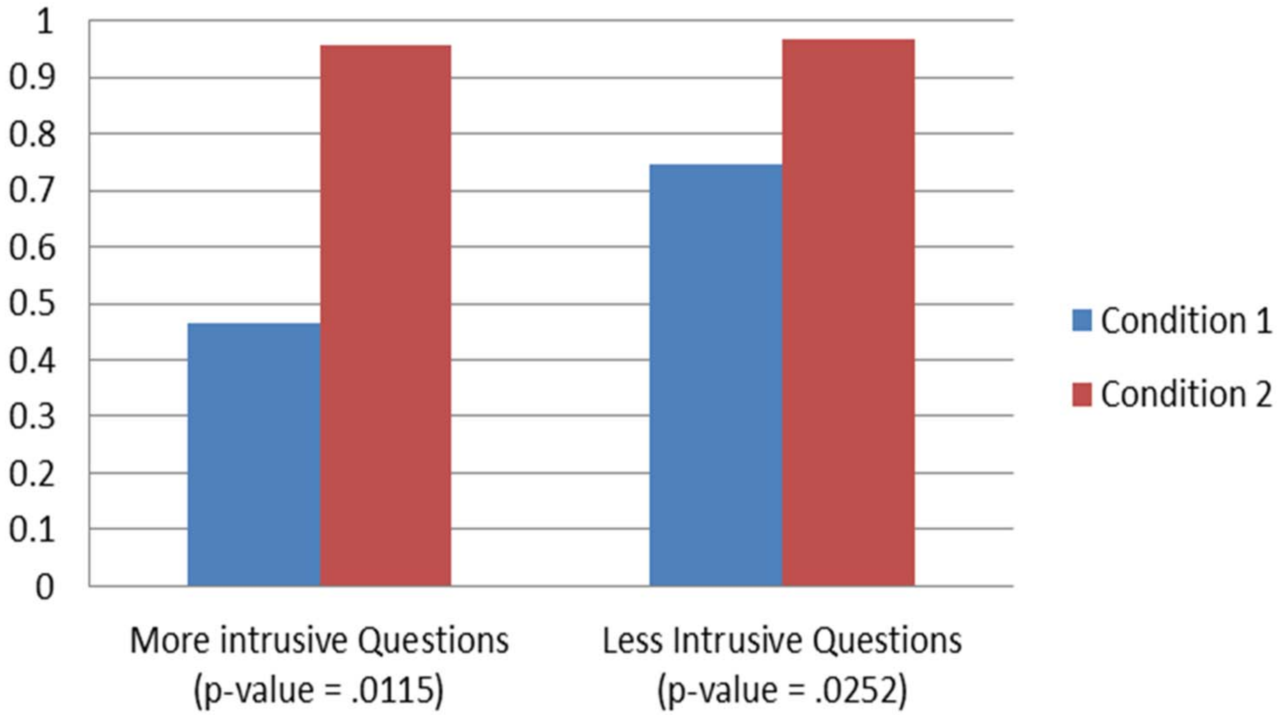
- Conditions (reduced)
  - **Implicit control condition (Condition 1)**

    "All answers are voluntary. By answering a question, you agree to give the researchers permission to publish your answer."
  - **Explicit control condition (Condition 2)**

    "All answers are voluntary. In order to give the researchers permission to publish your answer to a question, you will be asked to check the corresponding box in the following page."

Results

Average Publication Rates



Manipulation checks

- Exit questionnaire focus on:
  - Perceived control
  - Privacy sensitivity
- Mediation analysis based on exit questionnaire strongly supports our interpretation of the results:
  - Higher perceived control decreases privacy concerns (and increases self-disclosure) even when actual accessibility by strangers to one's personal information increases

Implications

- It is not just the publication of private information *per se* that disturbs people, but the fact that someone else will publish it for them
- Results call into questions OSNs' arguments of protecting privacy by providing more control to members
  - *Giving more control to users over information publication seems to generate higher willingness to disclose sensitive information*

Four studies

1. The inconsistency of privacy valuations
2. The paradox of control
3. **Discounting past information**
   - **With Laura Brandimarte and Joachim Vosgerau**
4. Faces of Facebook: Privacy and face recognition

Research question

- Premise: Internet as the end of forgetting
- How does information about a person's past, retrieved today, get 'discounted'?
  - Specifically: does information about a person's past with **negative valence** receive more weight in impression formation than information with **positive valence**?

Hypothesis

- Impact of information with negative valence lasts longer than impact of info with positive valence, not merely because of asymmetric effects of valence or memory effects, but also because of different weights (discount rates) applied to the two types of info

- This may be due to
  - Mobilization effects (Taylor 1991) and evolutionary theory (Baumeister et al. 2001)
  - Negativity bias (Seligman & Maier 1967)
  - Negative information is more attention grabbing (Pratto & John 1991)

Four randomized experiments

- We ran three survey-based randomized experiments, and one actual experiment, manipulating **valence** of information about third parties provided to subjects and the **time** to which that information referred
- Subjects were asked to express a judgment on the person or company they just read about
- Three experiments:
  - The dictator game (survey version and version with real incentives)
  - The company experiment
  - **The wallet experiment**

Experimental conditions

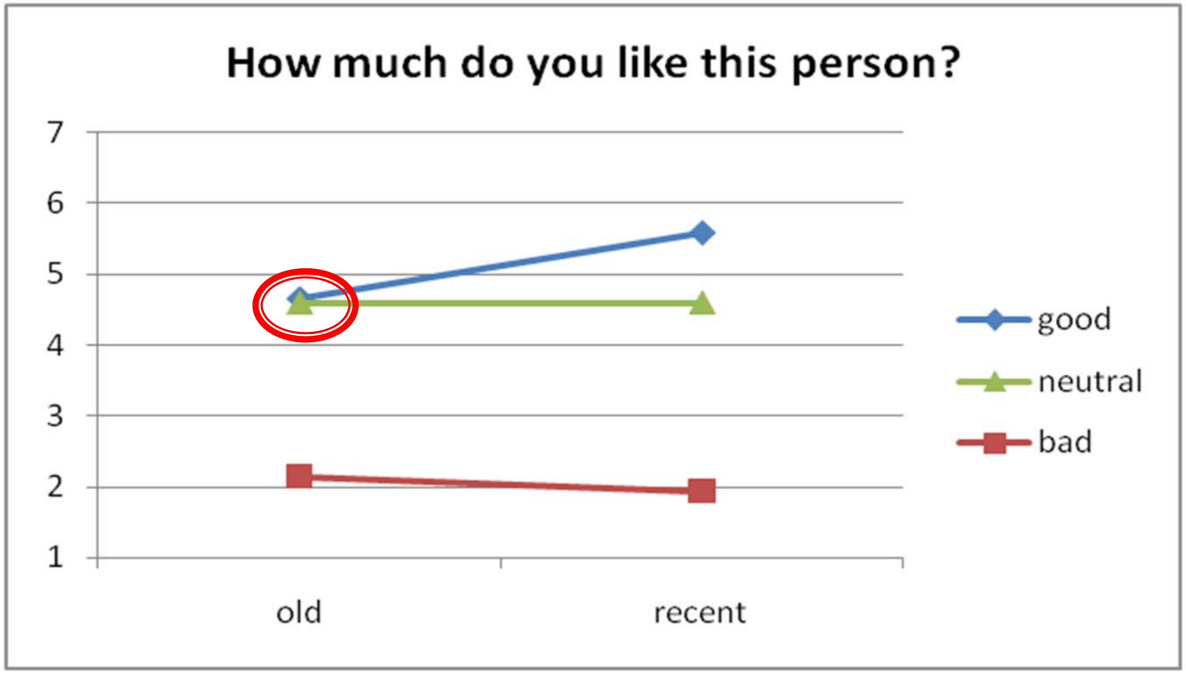
- To summarize:
  - One “neutral” baseline condition
  - 2x2 “treatment” conditions with additional positive/negative information:

Reported wallet, 5 years ago	**Reported wallet, 12 months ago**
Did not report wallet, 5 years ago	**Did not report wallet, 12 months ago**

Dependent variables

- Dependent variables:
  - **How much subjects liked the person described**
  - How much they trusted the person described
  - How much they would like to work with her

Results


How much do you like this person?
7
6
5
4
3
2
1
old
recent
good
neutral
bad

Implications

- Bad is not just stronger than good…
- …. It is also discounted differently than good
- Implications: future impact of information revealed today

Overall implications of these behavioral privacy studies

- People's concerns for privacy (and security) depend, in part, on priming and framing
  - This does ***not*** necessarily mean that people don't care for privacy, or are "irrational," or make wrong decisions about privacy
- Rather, it implies that reliance on "revealed preferences" argument for privacy may lead to sub-optimal outcomes if privacy valuations are inconsistent…
  - People may make disclosure decisions that they stand to later regret
  - Risks greatly magnified in online information revelation

Four studies

1. The inconsistency of privacy valuations
2. The paradox of control
3. Discounting past information
4. Faces of Facebook: Privacy and face recognition
   - With Ralph Gross and Fred Stutzman

Face recognition: Background

- Computer face recognition has been around for a long time (e.g.: Bledsoe, 1964; Kanade, 1973)
- Computers still perform much **worse than humans** when recognizing faces
- However, automatic face recognition has consistently improved, and has started being used in production applications
  - Especially in security, and – more recently – Web 2.0

Face recognition: Background

- Face recognition in Web 2.0
  - Google has acquired Neven Vision, Riya, and PittPatt and deployed face recognition into Picasa
  - Apple has acquired Polar Rose, and deployed face recognition into iPhoto
  - Facebook has licensed Face.com technology to enable automated tagging
- *So, what is different about our research?*

What is different: The convergence of various technologies (1/2)

- Increasing **public self-disclosures** through **online social networks** - especially, photos
  - In 2000, 100 billion photos shots worldwide
  - In 2010, 2.5 billion photos uploaded by Facebook users alone *per month*
  - Often, through **identified** profiles
- Continuing **improvements** in face recognizers' accuracy
  - In 1997, the best face recognizer in FERET program achieved a false reject rate of 0.54 (at false accept rate of 0.001)
  - By 2006, the false reject rate was down to 0.01

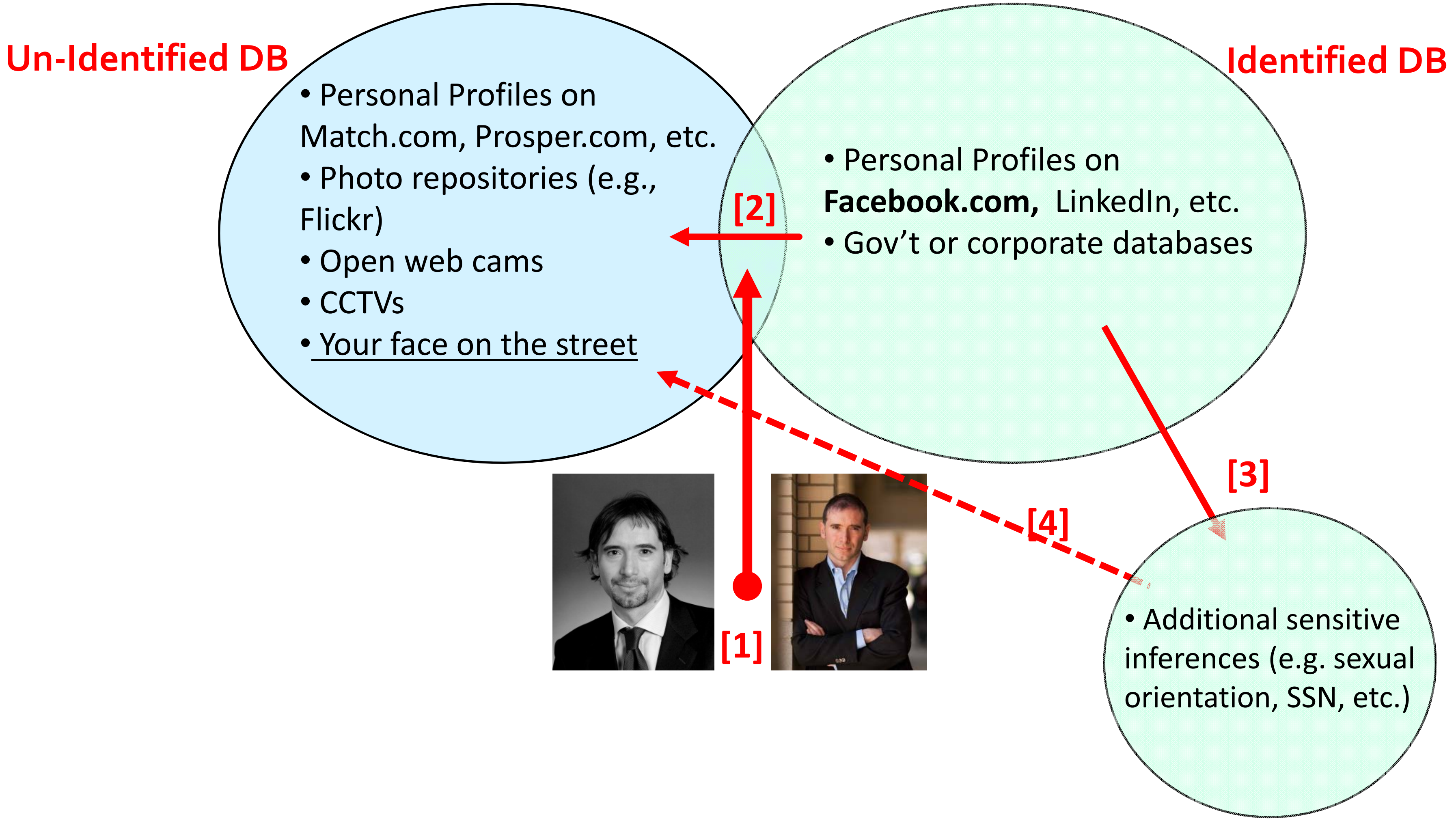
What is different: The convergence of various technologies (2/2)

- Statistical **re-identification:** sensitive inferences from public data
  - US citizens identifiable from zip, DOB, gender (Sweeney, 1997); Netflix prize de-anonymization (Narayanan and Shmatikov, 2006); SSN predictions from Facebook profiles (Acquisti and Gross, 2009)
- **Cloud** computing
  - Makes it feasible (and economic) to run millions of face comparisons in seconds
- **Ubiquitous** computing
  - Combined with cloud computing, makes it possible to run face recognition through mobile devices – e.g., smartphones

Our research focus

- Combining **publicly available** online social network data with **off-the-shelf** face recognition technology for the purpose of **large-scale, automated, peer-based…**
  1. **Individual re-identification**, online and offline
  2. **Inference** of additional, and potentially **sensitive, personal data**

In a nutshell



Un-Identified DB

- Personal Profiles on Match.com, Prosper.com, etc.
- Photo repositories (e.g., Flickr)
- Open web cams
- CCTVs
- Your face on the street

Identified DB

- Personal Profiles on **Facebook.com,** LinkedIn, etc.
- Gov't or corporate databases

- Additional sensitive inferences (e.g. sexual orientation, SSN, etc.)

Why Facebook?

- The issue we investigate is broader than Facebook.

  However:

  - FB Primary profile photos visible to all by default

    ``*Facebook is designed to make it easy for you to find and connect with others. For this reason, your name and profile picture do not have privacy settings*''

    (Facebook Privacy Policy)

  - Most FB members use photos of themselves as primary profile image
  - Most FB members use real first and last names on their profiles

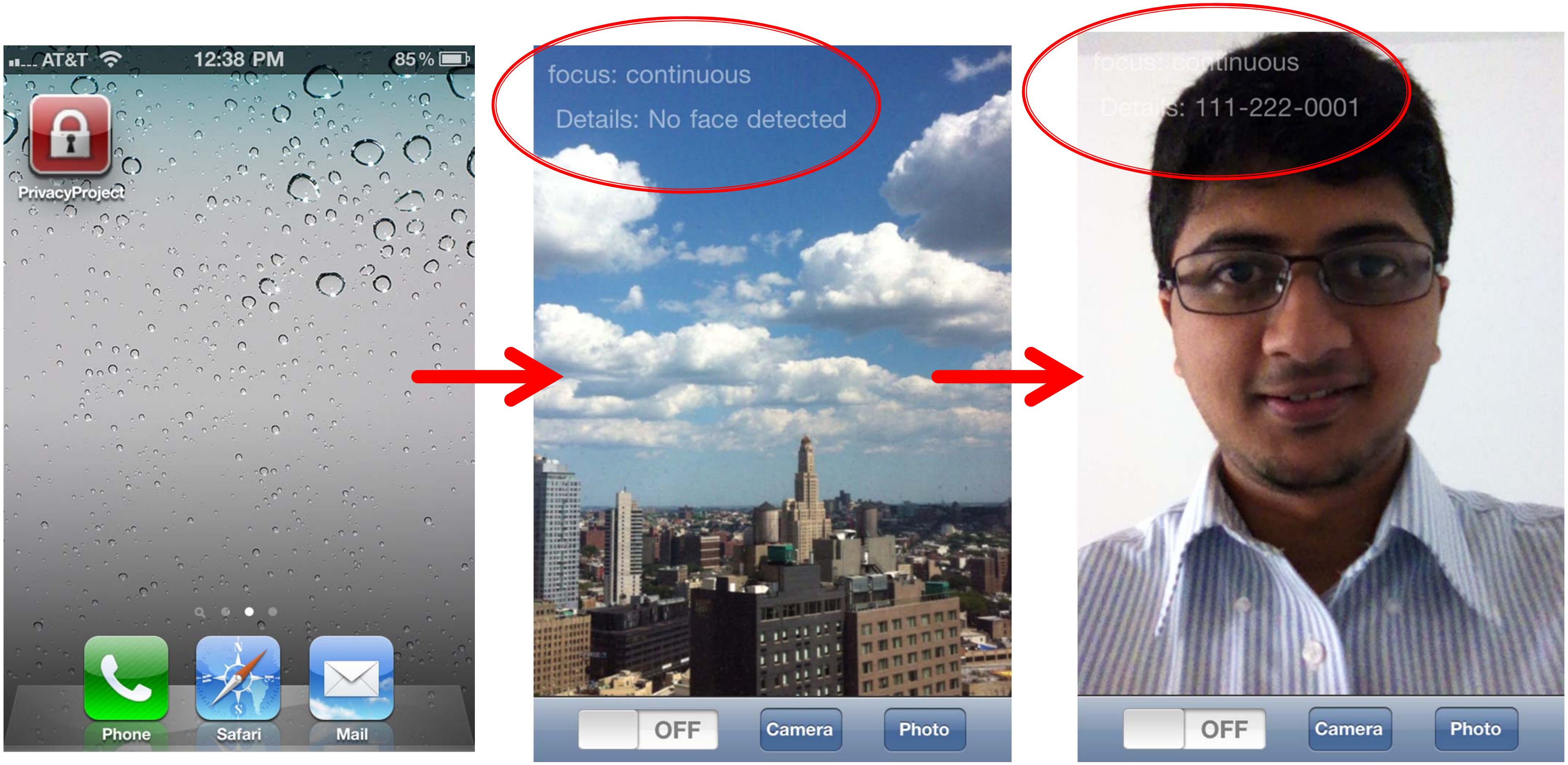
Experiments

- Experiment 1: Online-to-Online Re-Identification
- Experiment 2: Offline-to-Online Re-Identification
- Experiment 3: Offline-to-Online Sensitive Inferences

Real time demo

- We developed a demo smart phone app to combine and extend the previous experiments, allowing:
  - Personal and sensitive inferences
  - From someone's face
  - In real time
  - On a mobile device
  - **Overlaying information (obtained online) over the image of the individual (obtained offline) on the mobile device's screen**

Screenshots



focus: continuous

Details: No face detected

focus: continuous

Details: 111-222-0001

Limitations

- Availability of facial images
  - Legal and technical implications of mining identified images from online sources
- Cooperative subjects
  - Face recognizers perform worse in absence of clean frontal photos
  - On the street, clean and frontal photos of uncooperative strangers are unlikely
- Geographical restrictions
  - Experiment 1 focused on City area (~330k individuals). Experiment 2 focused on College community (~25k individuals)
  - As the set of potential targets gets larger (e.g., nationwide), computations needed for face recognition get less accurate (i.e., **more false positives**), and take more time

Extrapolations

- Face recognition of everyone/everywhere/all the time is **not** yet feasible
- **However:** Current technological trends suggest that most current limitations will keep fading over time

Implications

- These technologies challenge our expectations of **anonymity in a digital or a physical crowd**
- Especially risky, because:
  1. We do not anticipate being identified by strangers in the street/online
  2. We do not anticipate the sensitive inferences that can be made starting merely from a face
  3. No obvious solutions without risks of significant unintended consequences

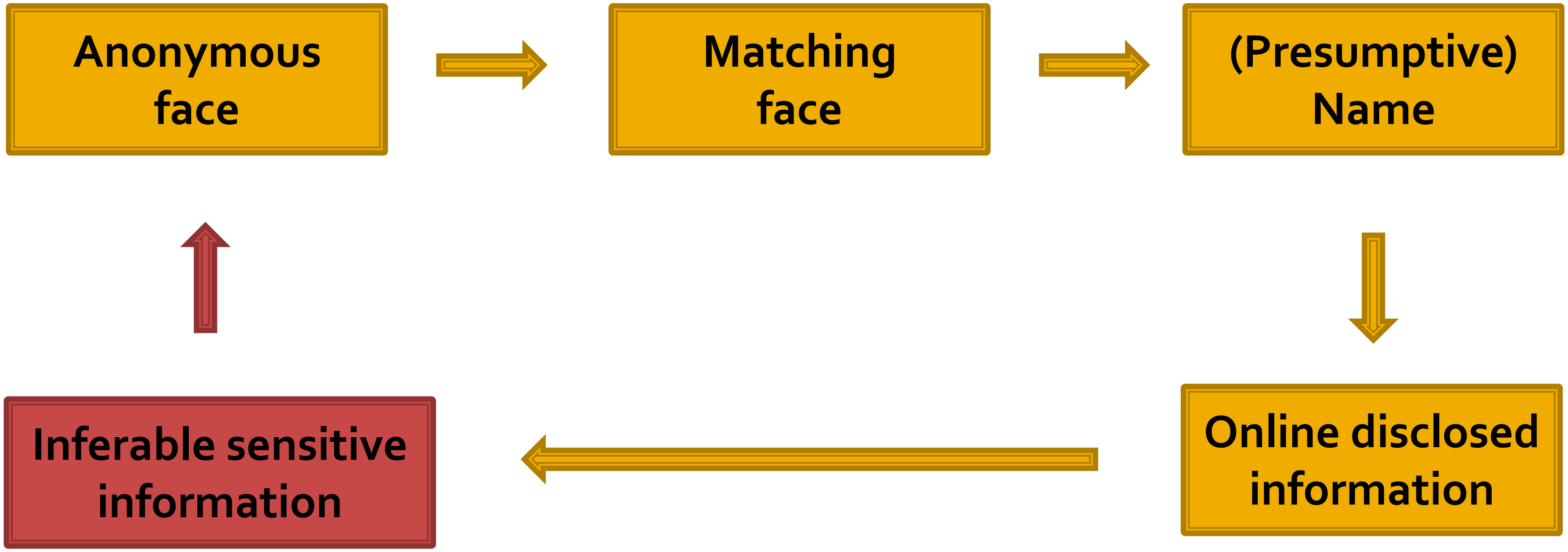
The key message

- Faces as conduits between online and offline data
- The emergence of PPI: “personally predictable” information
- Social network profiles as Real IDs
- The rise of visual, facial searches
- Democratization of surveillance
- The future of privacy in a world of augmented reality

Privacy in the age of augmented reality

- What **will privacy mean** in a world where a stranger on the street could guess your name, interests, SSNs, or credit scores?
  - The coming **age of augmented reality, in which online and offline data are blended in real time**, may force us to reconsider our notions of privacy

Data “accretion”



Anonymous face

Matching face

(Presumptive) Name

Online disclosed information

Inferable sensitive information

Behavior in the age of augmented reality

- In fact, this “augmented reality” may also carry **deep-reaching behavioral implications**
  - Through natural evolution, human beings have **evolved mechanisms to assign and manage trust in face-to-face interactions**
  - Will we rely **on our instincts, or on our devices**, when mobile devices make their own predictions about hidden traits of a person we are looking at?

For more info

- Google: economics privacy
- Visit: http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm
- Email: acquisti@andrew.cmu.edu