Introduction to Privacy Technologies

Claudia Diaz
KU Leuven – COSIC

Croatia, June 2015

News › World news › US national security

Series: Glenn Greenwald on security and liberty

NSA Prism program taps in to user data of Apple, Google and others

- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program 2007

Facebook tracks users without consent, breaks law

Daycare Worker Fired For Candid Facebook Post

The Huffington Post | Dominique Mosbergen | Posted 05.05.2015 | **Business**

Read More: Daycare Worker Fired Facebook, Fired Over Facebook Post, Facebook, Social Media, Facebook Privacy, Single Mom Fired Facebook Post, Kaitlyn Walls Face

If you needed a reminder about watching what you post on social media, here's yet another cautionary tale. According to reports this week, a woman i...

Read Whole Story

Facebook

Facebook a top cause of relationship trouble, say US lawyers

Social networking site becoming primary source of evidence in divorce proceedings and custody battles, lawyers say

Community Health Systems hacked, 4.5M patients' information compromised

Written by Akanksha Jayanthi (Twitter | Google+) | August 18, 2014

38 Tweet 50

Franklin, Tenn.-based Community Health Systems h
people, according to an SEC regulatory filing issued

Hackers allegedly access
patients who were referre
according to the filing.

How did my dad's Uber account get hacked?

By Tom Heyden

GCHQ taps fibre-optic cables for secret access to world's communications

Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them with NSA, latest documents from Edward Snowden reveal

Privacy Technologies

- Aim to address / mitigate certain privacy concerns
  - While allowing us to enjoy the benefits of modern ICTs

- We distinguish three categories of technologies and discuss:
  - The privacy concerns they address
  - Their goals
  - Example technologies
  - Challenges and limitations

“Social privacy”: Privacy concerns

- Technology mediation of social interactions leading to problems in the immediate social context of the user
  - “My parents discovered I’m gay”
  - “My boss heard me say he’s an asshole”
  - “My friends saw my naked pictures -- OMG!”
- Self-presentation and identity construction towards friends, family, colleagues
  - Tension between privacy and publicity
- Decision making: cognitive overload, bounded rationality, immediate gratification, behavioral biases, …
- **Who** defines the privacy problem:
  - Users

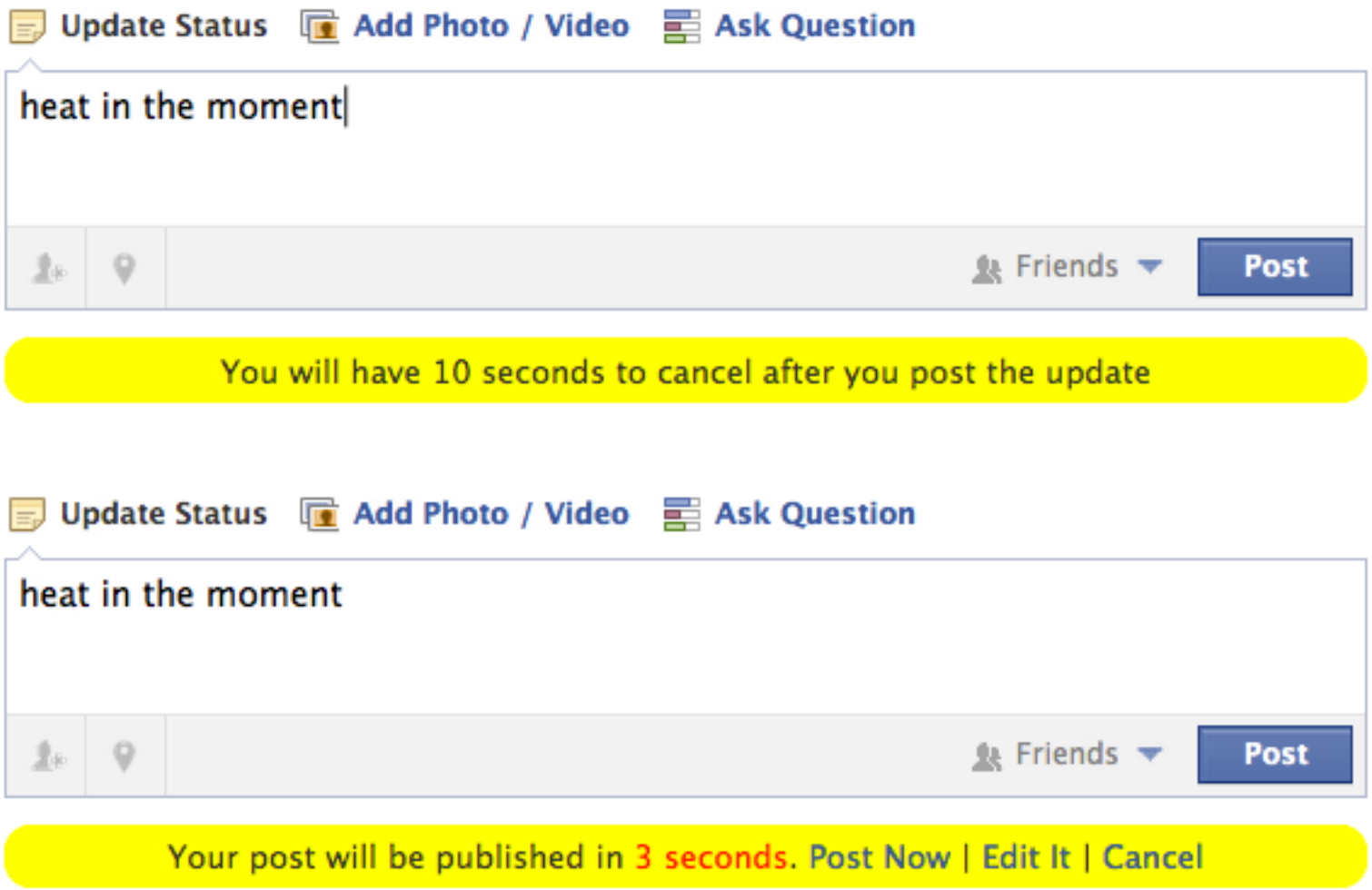
“Social privacy”: Goals

- Meet **privacy expectations**: system behaves as expected by the user:
  - *“don’t surprise the user!”*
- Make **privacy controls** (e.g., settings) visible and easy to use
- Assist users in privacy-relevant **decision making**:
  - users can predict the outcomes of their actions, such that they do not **regret** their actions after the fact
- Help users develop appropriate **privacy practices**
  - e.g., etiquette: use “Bcc:” instead of “Cc:” when sending email to a large number of people

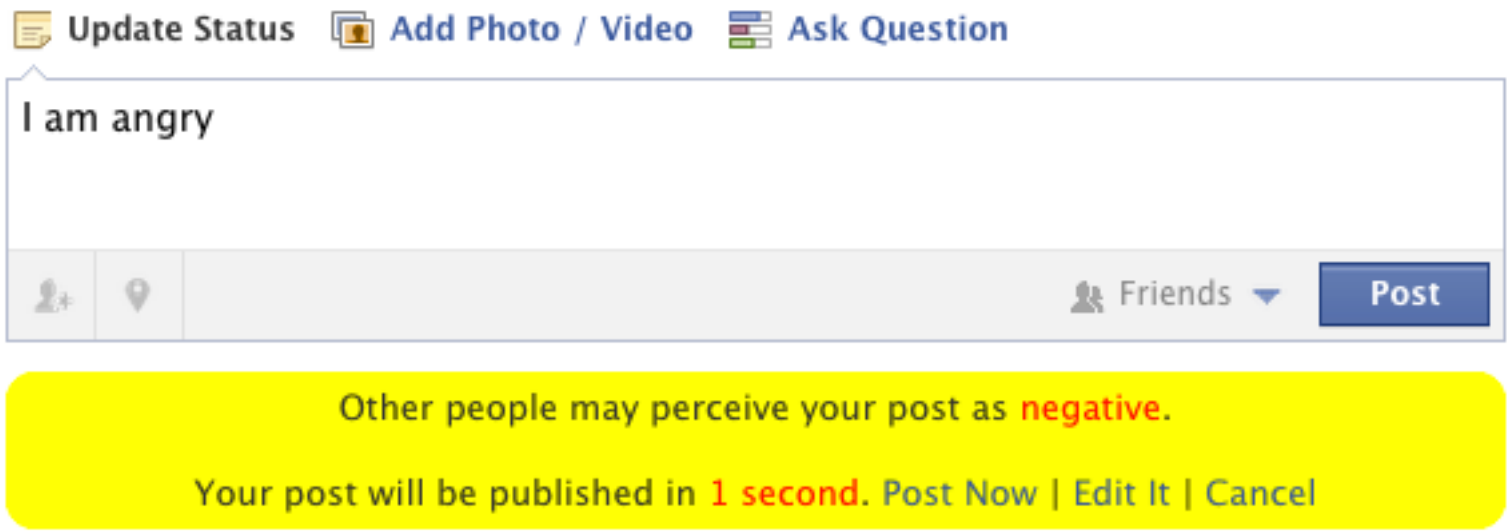
“Social privacy”: Examples

- Appropriate defaults
  - “only friends”
- Usable privacy settings, tools for audience segregation
  - automated grouping of friends
- Contextual feedback mechanisms
  - “how others see my profile”
- *Privacy nudges*

Timer nudge (stop and think)



Sentiment nudge (content feedback)



Social privacy technologies: challenges and limitations

- Focus on volitional actions and user-generated content
- Focus on the front-end
- Research methodology: user studies
  - Limited by users' understanding and perception of the system
  - Studies mostly conducted in Europe and North America
  - Focus on the "average consumer"
- Focus on "privacy expectations"
  - Slippery slope if expectations erode
- Paradox of control (affects all types of privacy technologies)

- Incentives for deployment:
  - Aligned with industry's interests: make users comfortable with sharing information in their systems

“Institutional privacy”: Privacy concerns

- Concerns mainly interactions with organizations
- Data collection without user awareness or *informed consent*
- **Use** of data for illegitimate purposes
- Sharing personal data with third parties
- Database breaches with personal data
- Account hijacking
- Data correctness, integrity, deletion
- **Who** defines the privacy problem:
  - Legislation, organizations (through policies)

“Institutional privacy”: Goals

- Ensure compliance with data protection principles:
  - informed consent
  - purpose limitation
  - data minimization
  - subject access rights

- Data security:
  - prevent (or mitigate the consequences of) data breaches
  - protect user accounts

- Auditability and accountability

“Institutional privacy”: Examples

- appropriate defaults and privacy controls
  - again, but here towards organizations instead of peers
- tools to make privacy policies easier to understand and negotiate
  - P3P, DNT
- tools to help organizations define and enforce access control policies
  - purpose-based access control
- auditing systems
- database privacy technologies

Institutional privacy technologies: challenges and limitations

- The organization is (semi-)trusted to be honest, competent, and act in the best interest of the user
  - Reliance on the legal system to punish lack of compliance
  - No (technical) protection guarantees towards organizations that want to violate user privacy by stealthily abusing the data that they hold
- Focus on limiting (mis)use of personal data, rather than collection
  - Does not preempt the creation of large databases
  - Auditing and legal compliance mechanisms may result in more data being recorded
- Who has the power to define and enforce the policies on data use?
  - Do whatever we wanted to do with the data while being compliant
- Focus on "personal data"
  - Does not address inferences from anonymized or aggregated data
- Limits on transparency posed by IP (proprietary software, algorithms, databases)

- Incentives for deployment: strong
  - Legal compliance is a very strong driver

Anti-surveillance technologies (PETs): Privacy concerns

- Data disclosure by default through the use of the ICT infrastructure
- Threat model:
  - surveillance by (possibly colluding) service providers and governments
  - censorship
- Relationship to other democratic values:
  - Protection of dissent, free speech, freedom of association, freedom from government intrusion, protection of the democratic system itself
- **Who** defines the privacy problem:
  - Security experts (techno-centric)

Anti-surveillance technologies (PETs): Goals

- Limit disclosure: prevent/minimize default **disclosure** of personal information to service providers and other third parties:
  - Only information *explicitly* disclosed is made available to *intended* recipients (confidentiality)
  - This includes user-generated content *and* implicit data

- Minimize the need to trust others with appropriately handling data
  - Distribute trust by avoiding single points of failure
  - Transfer of trust to the technology (protocols, software, hardware) itself:
    - need for **transparency**, availability of designs and implementations for public review

- Circumvent censorship
  - Availability properties
  - Circumvention might need to be undetectable (hard!)

Anti-surveillance technologies (PETs): Examples

- Protecting content: end-to-end encryption
  - PGP, OTR
- Protecting identity: systems for anonymous communications
  - Tor
- Advanced crypto protocols:
  - anonymous authentication
  - private information retrieval
  - private search
  - privacy-preserving smart metering
- obfuscation approaches:
  - TMN: degrade data quality with noise
- Technologies that expose surveillance (transparency)
  - FPDetective

Anti-surveillance technologies (PETs): challenges and limitations

- Focus on (preventing) data disclosure
  - No protection for information *after* disclosure
- Making secure design and implementations is hard
  - Importance of public algorithms and open source: "it takes a village to keep systems secure"
  - Security of end-devices: big issue
- Research methodology:
  - Narrow privacy definitions
  - Driven by threat (adversarial) models
  - Explicit (sometimes implicit) assumptions that need to hold to guarantee privacy properties (mathematical, behavioral, available building blocks, trust assumptions)
- Making security usable is hard
- Incentives for deployment: weak at best
  - Companies don't want this: less data is bad for business
  - Governments neither: national security, law enforcement, social control, detection of fraud
  - Who has to implement it? commercial SP, user (unilaterally), community

Conclusions

- Diverse landscape of privacy technologies, in terms of goals, limitations, and assumptions
  - hard to approach for outsiders (and even for insiders!)
- Importance of understanding embedded concepts of privacy and *who* gets to define those concepts and fill them with meaning!
- How to integrate the different technological approaches?
- Incentives!! Particularly, how to incentivize and support the deployment of anti-surveillance technologies?
- Articles and contact info: http://homes.esat.kuleuven.be/~cdiaz/