

Privacy Research Paradigms in Computer Science

Seda Gürses
MCC / ILI/ ISTC Social Computing

NYU

	privacy protects things of type X.	about privacy of what?	body of literature
Subject	Actor(s) or Entity(ies) protected by privacy, i.e. <i>privacy protects agent X.</i>	'Whose privacy is at stake?'	Private space Myself, My Child Social Groups (e.g., teens) Roles (e.g., students)
Dimensions of Harm			
Action	The act or behavior that initiates or constitutes a privacy harm, i.e. <i>staring at him while he was dressing in the locker room violated his privacy.</i>	'What act violated privacy?'	Solove's 4 meta-harms (Collection, Processing, Dissemination, Invasion)
Offender	Actor(s) violating privacy, i.e. <i>privacy violated by agent X.</i>	'Who violated privacy?'	Government Business Entity Peeping Tom
From-Whom	Actor(s) against-whom privacy is a protection, i.e. <i>privacy provides protection against agent X.</i>	'Who is privacy protecting against?'	Everyone Government 'Friends or friends'
Dimensions of Provision			
Mechanism	That which instrumentally secures privacy, i.e. <i>the lock on her door protected her privacy.</i>	'How is privacy provided?'	Legal Regulations Technical Design Social Norms
Provider	Actor(s) charged with securing privacy, i.e. <i>the telecommunications provider was responsible for technically securing the privacy of her communications.</i>	'Who is supposed to provide privacy?'	Government Business Entity Technology
Expert	Actor(s) charged with determining	'Who knows what	Policymakers

solutions from privacy research

storage
privacy

anonymous
communications

database
anonymization

differential
Privacy

private
information
retrieval

discrimination aware
data mining

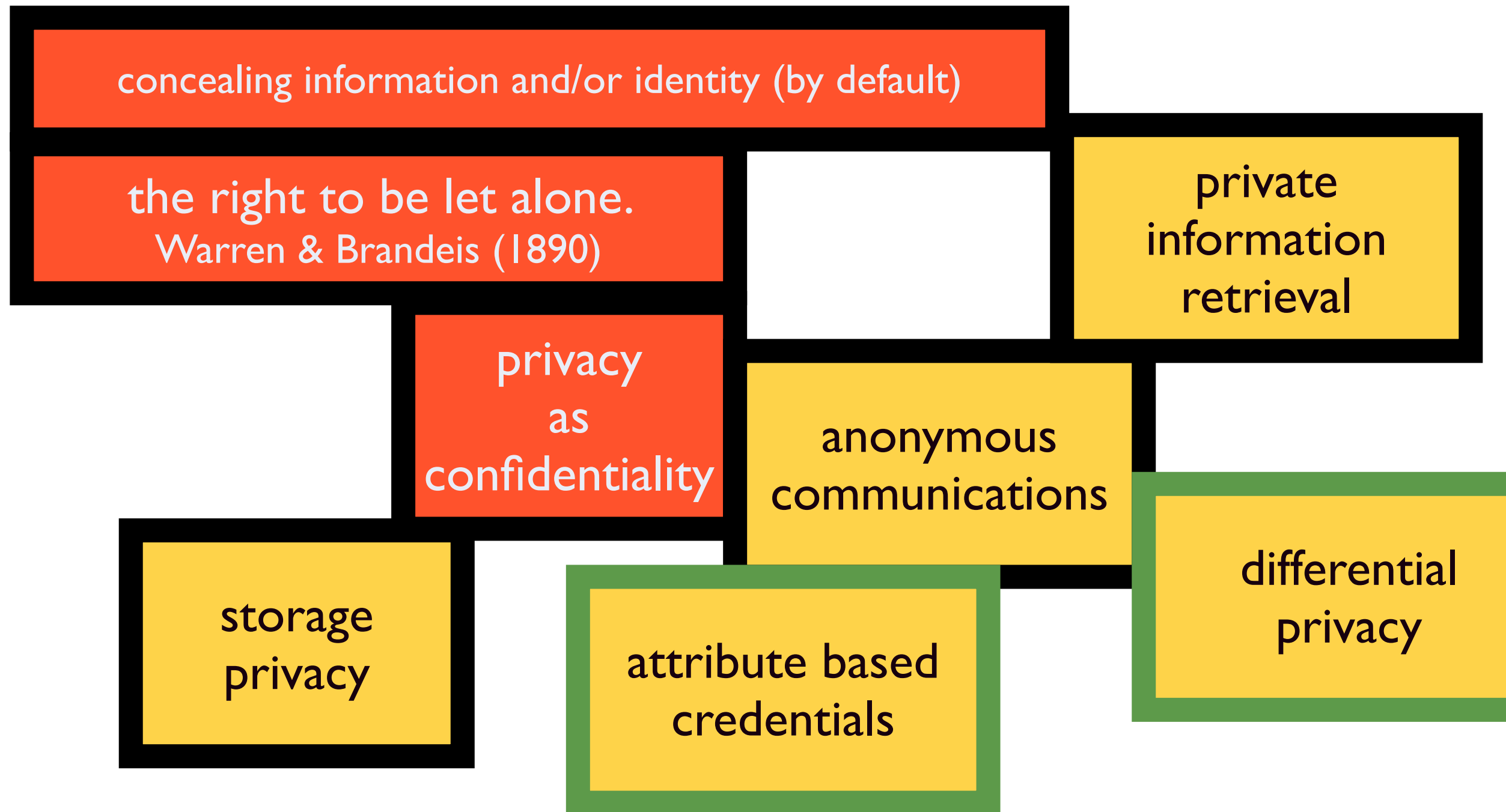
attribute based
credentials

IDMS

privacy policy
languages

Feedback and
Awareness
Systems

privacy research paradigms



privacy research paradigms

concealing information and/or identity (by default)

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

data minimization: every bit counts

distributed trust model: avoid single point of failure

open source: it takes a village to keep it secure

privacy research paradigms

concealing information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

right of the individual to decide
what information about himself
should be communicated to
others and under what
circumstances. (Westin 1970)

privacy
as control

personal
information,
FIPPs,
transparency

privacy research paradigms

database
anonymization

right of the individual to decide
what information about himself
should be communicated to
others and under what
circumstances. (Westin 1970)

IDMS

Privacy Policy
Languages

privacy
as control

FIPPs,
organizational
compliance, data
subject
participation

Privacy
Settings

Privacy
Labels/Signals

Purpose
Based Access
Control

privacy research paradigms

right of the individual to decide what information about himself should be communicated to others and under what circumstances. (Westin 1970)

privacy
as control

FIPPs,
organizational
compliance, data
subject
participation

(DHS) FIPPs

transparency

individual participation

data minimization (diff. trust model)

identity management

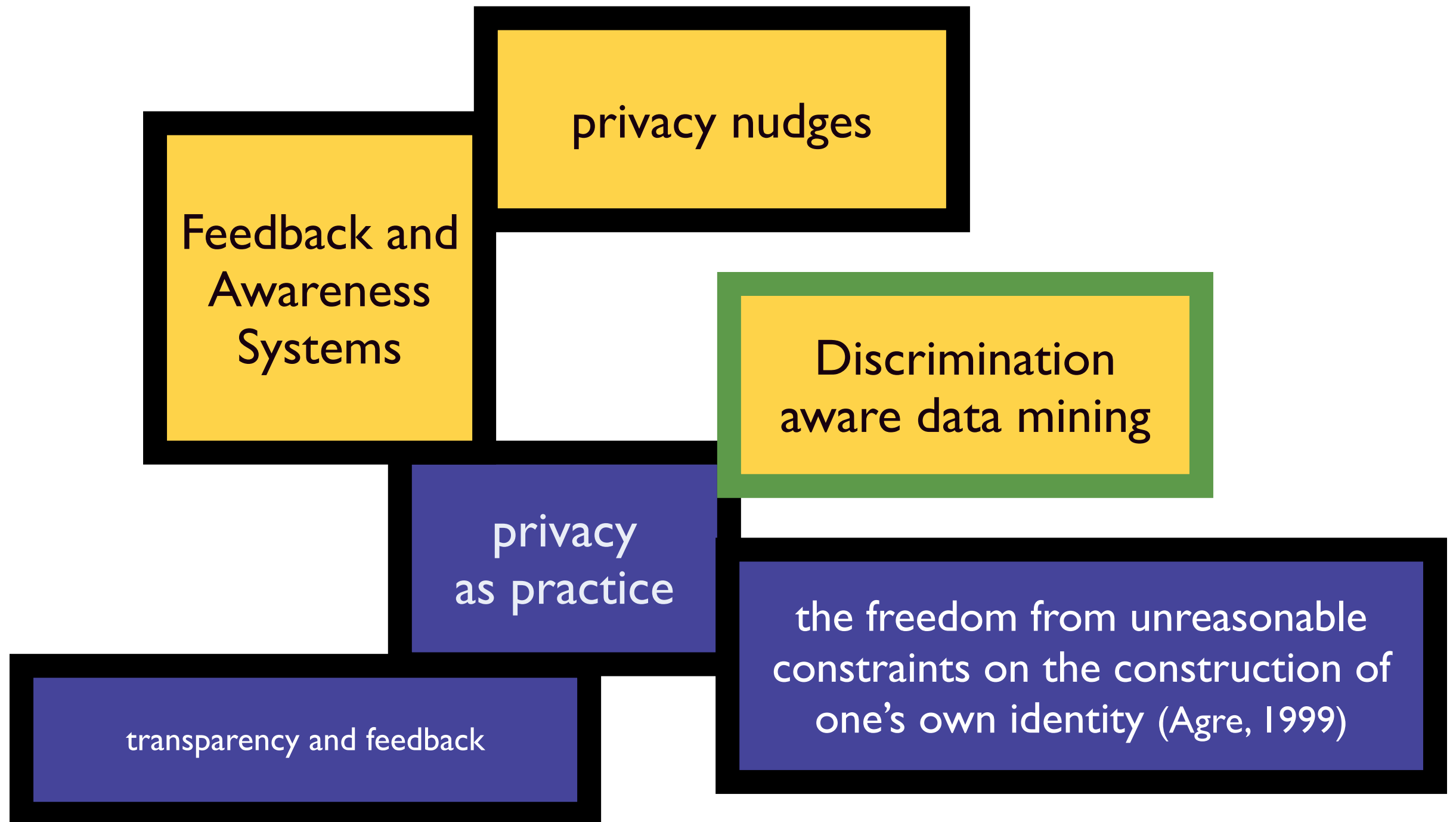


privacy policies

Bell Group

information we collect	ways we use your information				information sharing	
	to provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt in			opt out	
cookies						
demographic information		opt in			opt out	
financial information						
health information						
preferences						
purchasing information		opt in			opt out	
social security number & gov't ID						
your activity on this site		opt in			opt out	
your location						

privacy research paradigms



privacy research paradigms

support collective practices throughout time

aid in privacy decision making and nudges

salient controls according to user expectations

privacy
as practice

transparency and feedback

the freedom from unreasonable
constraints on the construction of
one's own identity (Agre, 1999)

Status Photo Place Life Event

What's on your mind?

Friends Post

Austin Kane shared a link.
8 December near Wilsonville, O

http://www.liveleak.com/view?i=1c3_1323325763

Lawlz dubstep cats.

 LiveLeak.com - Kittens waking up from painkillers after a visit to the vet.
www.liveleak.com
:-))

Are you sure you want to make
your photo public?

No Yes

slide: Lorrie Cranor

 Update Status  Add Photo / Video  Ask Question

heat in the moment|

   Friends ▼ [Post](#)

You will have 10 seconds to cancel after you post the update

 Update Status  Add Photo / Video  Ask Question

heat in the moment

   Friends ▼ [Post](#)

Your post will be published in **3 seconds**. [Post Now](#) | [Edit It](#) | [Cancel](#)

slide: Lorrie Cranor

 Update Status  Add Photo / Video  Ask Question

I am angry



 Friends ▼

Post

Other people may perceive your post as **negative**.

Your post will be published in **1 second**. [Post Now](#) | [Edit It](#) | [Cancel](#)

 Update Status  Add Photo / Video  Ask Question

this is a public post



Public ▼

Post



These people and **ANYONE ON THE INTERNET** can see your post.

privacy research paradigms

concealing information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

privacy
as practice

transparency and feedback

right of the individual to decide
what information about himself
should be communicated to
others and under what
circumstances. (Westin 1970)

privacy
as control

separation of
identities, FIPPs

the freedom from unreasonable
constraints on the construction of
one's own identity (Agre, 1999)

info privacy
legislation

dependent solely on service provider:
privacy settings on social network

service provider implements part:
private information retrieval
attribute based credentials

autonomous applications:
pgp
ghostery

privacy functionality dependency on service provider

collaborative applications:
distributed SNS
TOR
multi-party computation
open standards?

people-
centric

family

friends

communities

citizens

consumers

organization-centric

CRM

Facebook (as platform and app)

Hospital Management System

infrastructure/techno-centric

standard protocols

browsers

mobile phones

Thank you!

- seda@nyu.edu