At the Intersection of Ethics and Technology: Contextual Integrity and other Values

Helen Nissenbaum
New York University

NSF/CISE Distinguished Lecture
05|11|16 Arlington

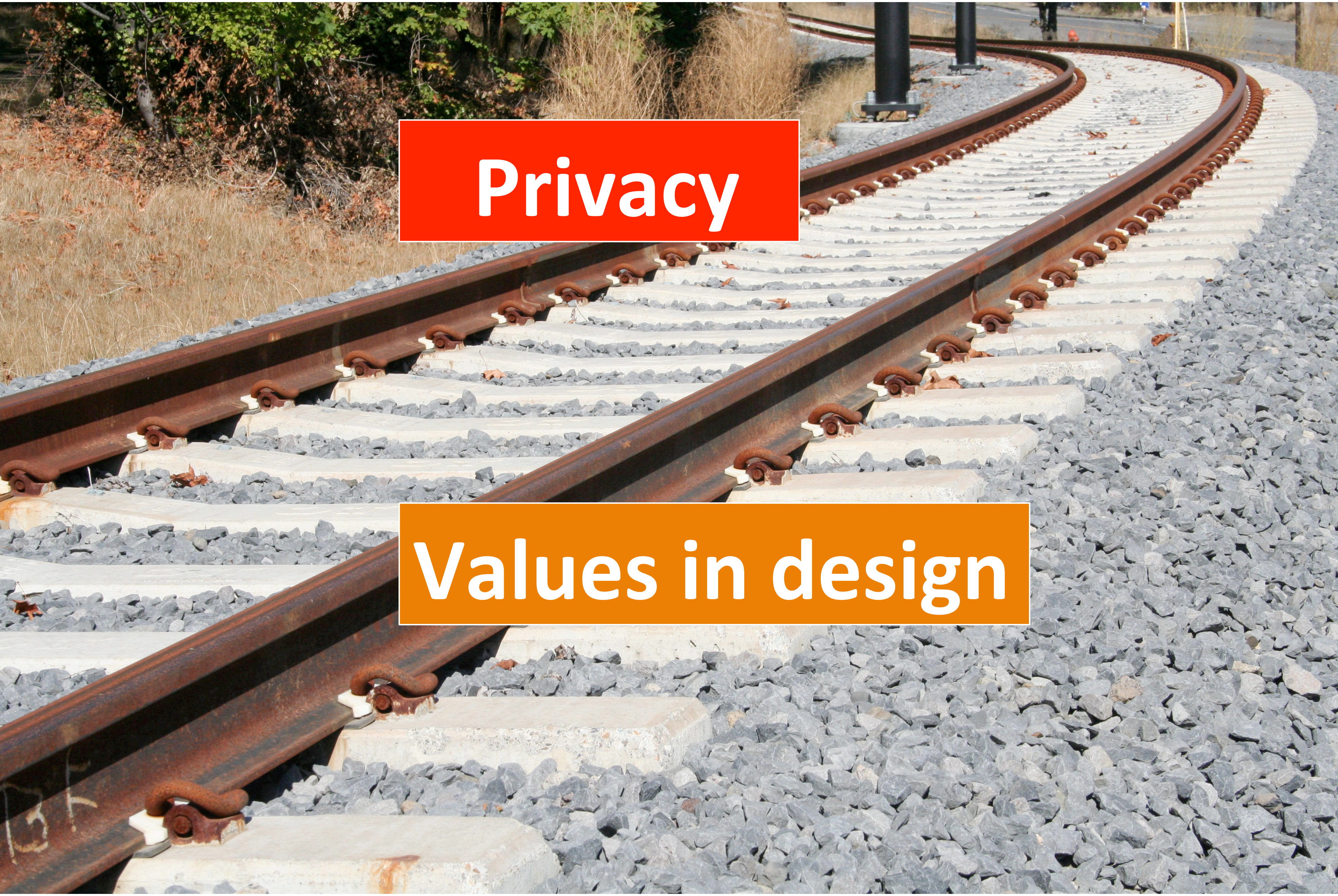
With support from:

- EAGER: Collaborative: A Research Agenda to Explore Privacy in Small Data Applications, 2015
- EAGER: Values in Design for Future Internet Architecture – Next Phase, 2014; EAGER: Values in Design in the Future Internet Architecture, CNS/ NetS 1058333, 2010
- Cyber-Trust (CT) Collaborative Research: CT-M: Privacy, Compliance and Information Risk in Complex Organizational Processes, CNS-0831124, 2008.
- Science of Design Collaborative Research: Values at Play – Integrating Social Factors into Design CNS 0613893, 200
- Collaborative Research: A Workshop on Values in the Design of Information Technology, SES-0352632, 2004,
- Collaborative Research: ITR-0331542: Sensitive Information in a Wired World, 2003
- SBR-9806234, Societal Values in an Age of Information Technology,1998
- SBR-9729447, Network Security Responsive to Human Values: Theory and Practice, 1998

Study of ethics and political philosophy of our time

+

computation and digital technologies



Privacy

Values in design

Outline

- Values in Design – Values at Play
- Privacy, digital IT, computation
- Contextual Integrity Fundamentals
- Policy , ethics, society, technology
- Solves some problem; more work to do
- On the horizon … (over the rainbow?)

Values in design

Where computer security meets national security

Securing trust online: wisdom or oxymoron

Accountability in a computerized society

Will computers dehumanize education? w/Walker

Bias in computer systems, w/Friedman

Values in Design

Commons based peer-production and virtue, w/Benkler

The politics of search engines: sustaining the public good vision of the Internet, w/Introna

New research norms for a new medium: The puzzle of priority

Ethical and political values in future Internet architecture (FIA)

Technique

Algorithm

Technical system

Socio-technical system

Protocol

Values in Technology

Architecture

Mechanism

Tool

Model

Design

The essence of VID

Ethical values emerge from technologies as they function within particular human, social settings.

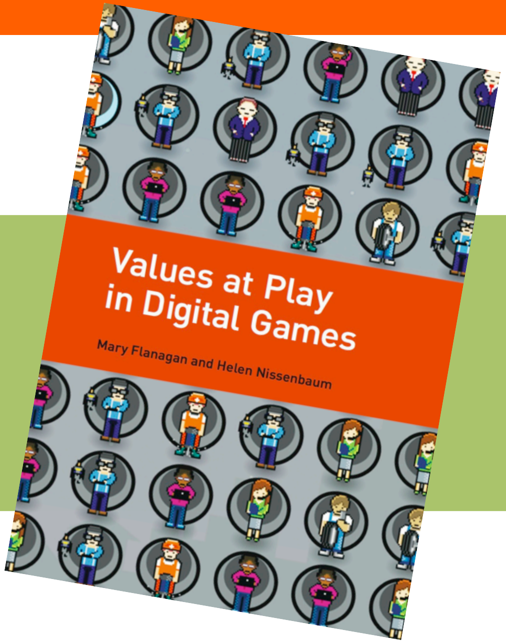
The belief that technical properties and ethical (political) properties can be made to “line up” in certain ways

“We are in this together”: looking back and being proactive

THE PRACTICAL TURN …

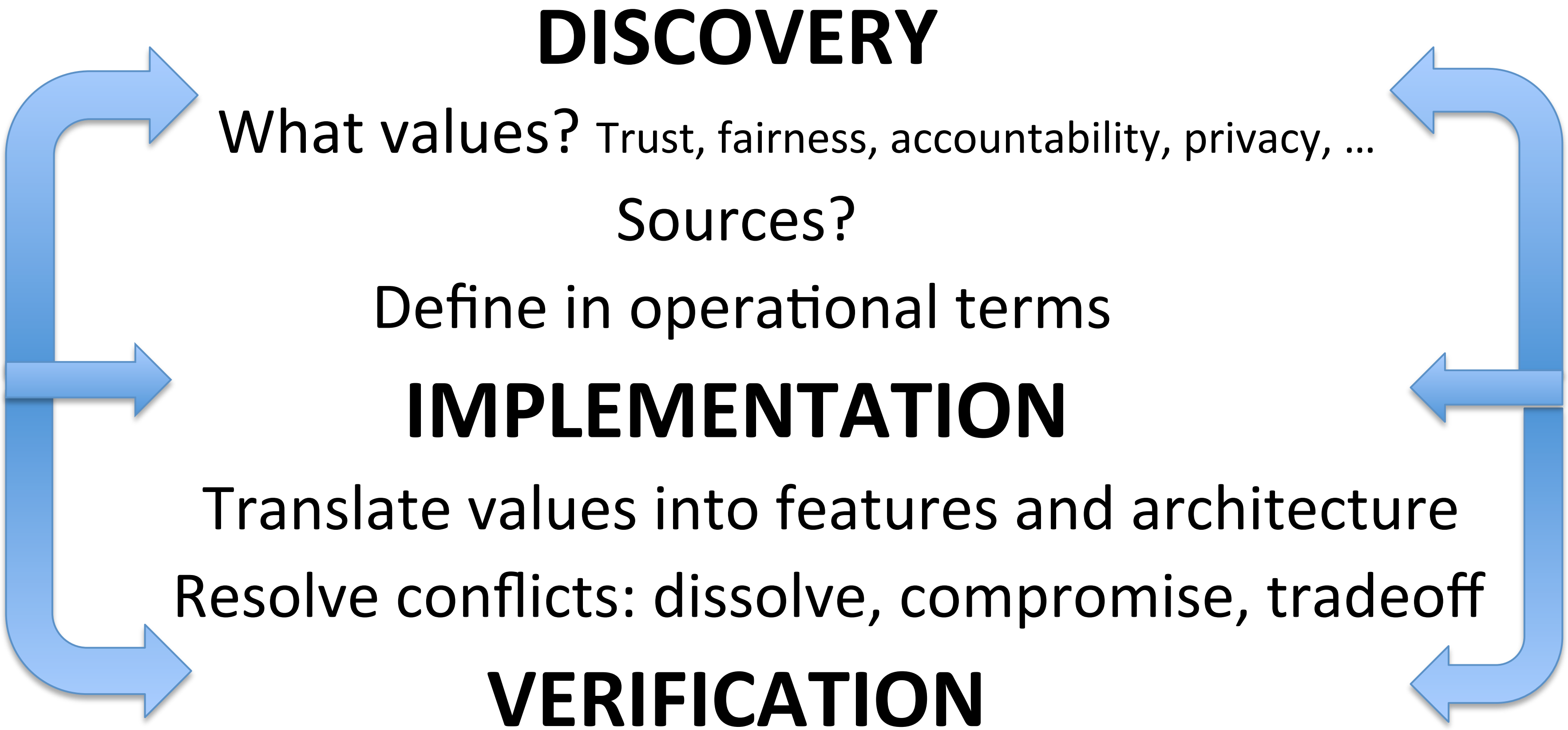
Values @ Play

Howe, Flanagan, Nissenbaum


Values at Play in Digital Games
Mary Flanagan and Helen Nissenbaum

Values @ Play

[Howe, Flanagan, Nissenbaum]



DISCOVERY

What values? Trust, fairness, accountability, privacy, …

Sources?

Define in operational terms

IMPLEMENTATION

Translate values into features and architecture

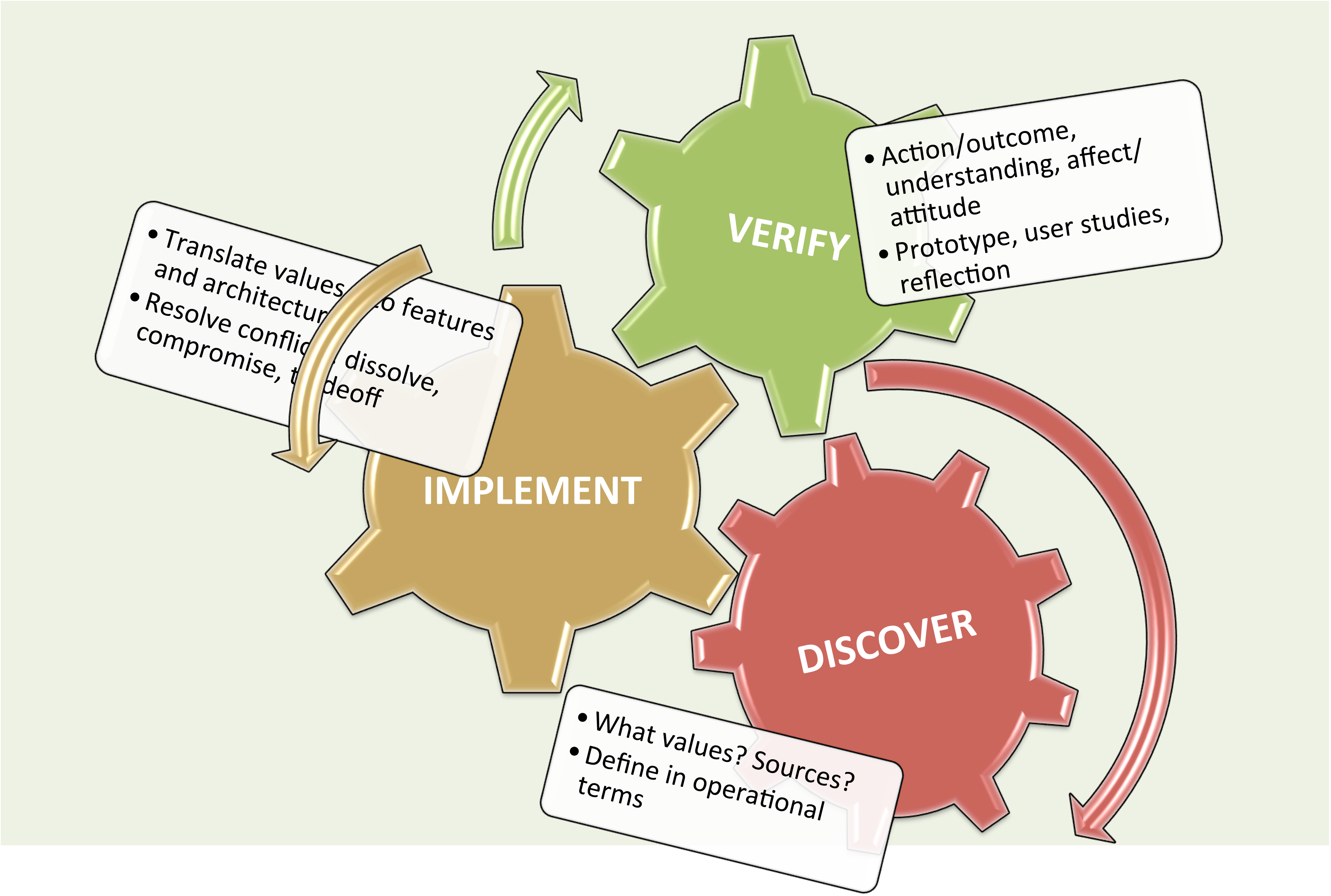
Resolve conflicts: dissolve, compromise, tradeoff

VERIFICATION

Action/outcome, understanding, affect/attitude

Prototype, user studies, reflection

Values @ Play



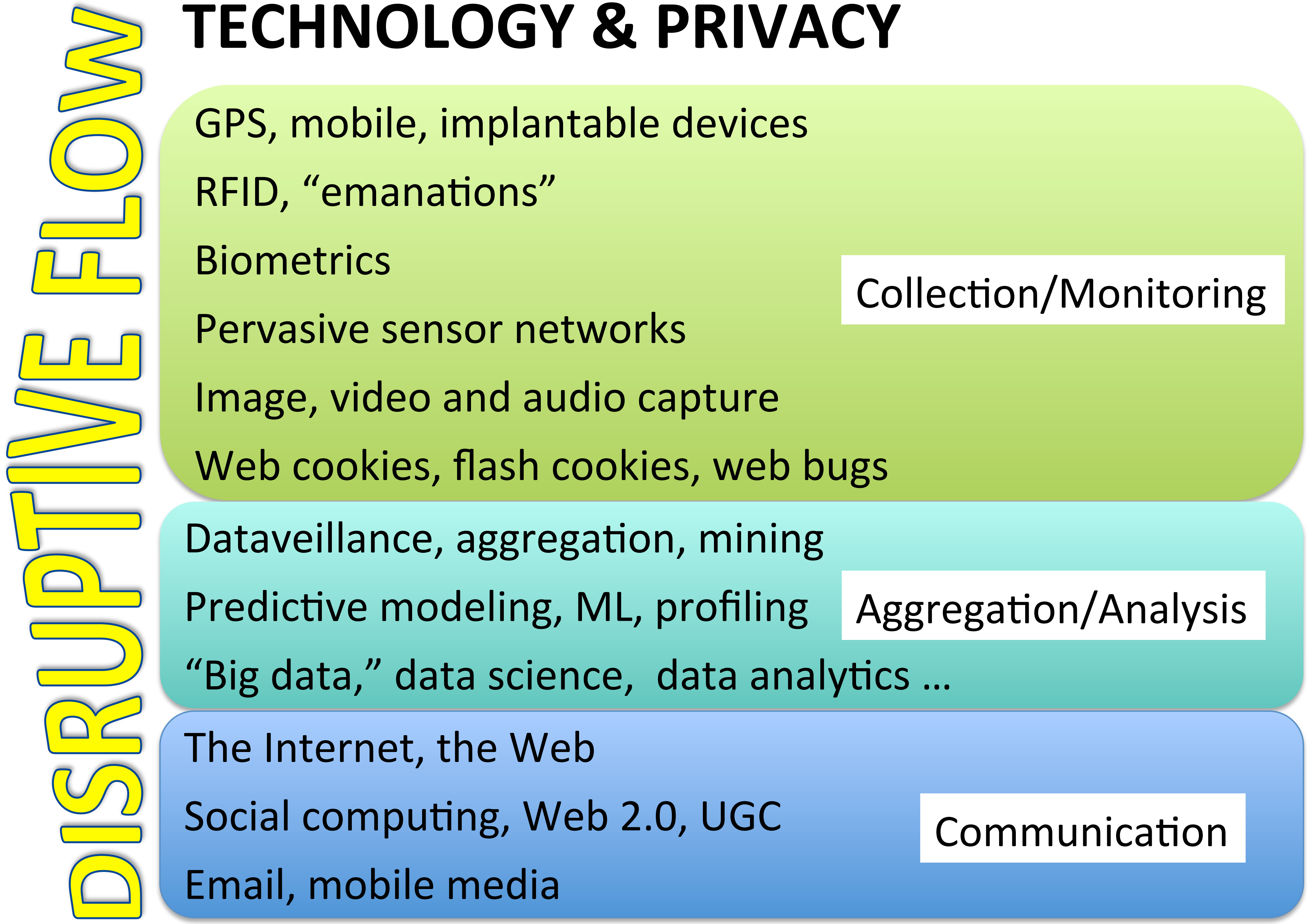
- What values? Sources?
- Define in operational terms

- Translate values to features and architecture
- Resolve conflict, dissolve, compromise, tradeoff

- Action/outcome, understanding, affect/ attitude
- Prototype, user studies, reflection

Privacy

TECHNOLOGY & PRIVACY



DISRUPTIVE FLOW

GPS, mobile, implantable devices

RFID, “emanations”

Biometrics

Pervasive sensor networks

Image, video and audio capture

Web cookies, flash cookies, web bugs

Collection/Monitoring

Dataveillance, aggregation, mining

Predictive modeling, ML, profiling

“Big data,” data science, data analytics …

Aggregation/Analysis

The Internet, the Web

Social computing, Web 2.0, UGC

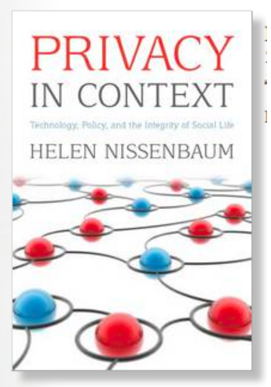
Email, mobile media

Communication

PRIVACY

"the problem of privacy in public" (1997)

Contextual Integrity Fundamentals



PRIVACY IN CONTEXT

Technology, Policy, and the Integrity of Social Life

HELEN NISSENBAUM

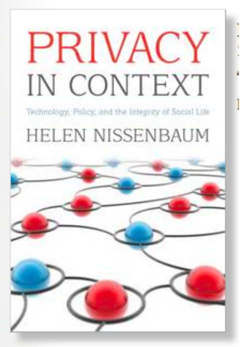
I. Privacy as appropriate flow

NOT

Information leakage as privacy violation

No-flow as privacy

Contextual Integrity Fundamentals

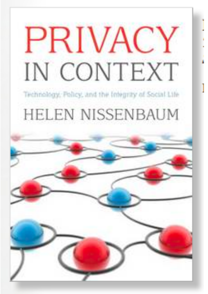


II. Appropriate flow as conformance with contextual informational norms

NOT

- Procedurally defined
  - Subject control over information
  - FIPPs
  - Informed consent

Contextual Integrity Fundamentals



III. Structure of contextual informational (privacy) norms -- five parameters: <subject, sender, recipient>, <information type>, <transmission principle>

NOT

Subject control

Public/Private

General vs. contextual norms

Access control rules specifying fewer than 5

ALL THE PARAMETERS MATTER!

Informational norms=Appropriate Flow

In a job interview, an interviewer is forbidden from asking a candidate's religious affiliation

A priest may not share congregants confession with anyone

A citizen of the U.S. is obliged to reveal gross income to the IRS, under conditions of confidentiality except as required by law

One may not share a friend's confidences with others, except, perhaps, with one's spouse

Parents should monitor their children's academic performance

Informational norms: Key Parameters

Actors

Sender

Recipient

Subject

Physician, merchant, bank, friend

Merchant, police, ad network

Patient, shopper, investor, reader

Information types

Demographic, biographical

Actions, communications

Medical status, financial

Transmission Principles

Consent, coerce, steal, buy, sell

Confidentially, stewardship

With a warrant, surreptitiously

Daisy Smith applies for a loan from Wells Fargo Bank. She authorizes Wells Fargo to obtain a credit report from Equifax

Equifax provides Daisy White's credit report to Wells Fargo Bank with authorization from Daisy White

sender

subject

Information type

recipient

Transmission principle

Flow analysis MUST specify ALL parameters: Sender, Subject, Recipient; Information types; Transmission principles

Informational Norms Embedded in Law: Example (GLB Act)

Barth, Datta, Mitchell, & Nissenbaum, "Privacy and Contextual Integrity: Framework and Applications," Proc. of the IEEE Symposium on Security and Privacy, May 2006.

Sender role Subject role

Financial institutions must notify consumers if they share their non-public personal Attribute information with non-affiliated companies, Recipient role *but the notification may occur either before or after the information sharing occurs*

Transmission principle

Exactly as **CI** says!

In our formal computer language,

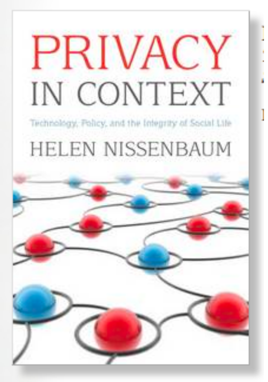
$$\Box \forall p_1, p_2, q : P. \forall m : M. \forall t : T.$$

$$\mathrm{incontext}(p_1, c) \wedge \mathrm{send}(p_1, p_2, m) \wedge \mathrm{contains}(m, q, t) \rightarrow$$

$$\mathrm{inrole}(p_1, \mathit{institution}) \wedge \mathrm{inrole}(p_2, \mathit{non\text{-}affiliate}) \wedge \mathrm{inrole}(q, \mathit{consumer}) \wedge (t \in \mathit{npi}) \rightarrow$$

$$\Diamond \mathrm{send}(p_1, q, \mathit{privacy\text{-}notice}) \vee \diamondminus \mathrm{send}(p_1, q, \mathit{privacy\text{-}n}$$

Contextual Integrity Fundamentals



IV. Ethical legitimacy of privacy norms is based on:

- Interests and preferences of affected parties
- Ethical and political principles and values
- Contextual functions, purposes, and values

NOT

Interests of data subject (Harm to the individual)
Tradeoff of principles and values (e.g. privacy vs. security)

Evaluating norms?

Contextual functions, purposes and values

healthcare: cure disease; alleviate suffering, equity …

political: democracy; freedom from exploitation …

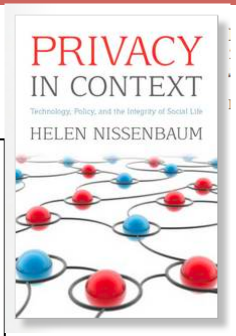
home and social: trust, autonomy, stability …

education: knowledge, intellect, fair distribution

“While the government does not know every source of income of a taxpayer and must rely upon the good faith of those reporting income, still in the great majority of cases this reliance is entirely justifiable, principally because the taxpayer knows that in making a truthful disclosure of the sources of his income, information stops with the government. It is like confiding in one’s lawyer.”

Secretary of the Treasury, Andrew Mellon, 1925

Contextual Integrity Fundamentals



I. Privacy as appropriate flow

II. Appropriate flow as conformance with contextual informational norms

III. Contextual informational (privacy) norms specify values for five parameters:
<subject, sender, recipient>,
<information type>, <transmission principle>

IV. Ethical legitimacy of privacy norms is based on: interests, ethical/political values,
+ contextual functions, purposes, and values

Policy

Social science and theory

CI: “testing its mettle”!

Ethics and philosophy

Science and technology

White House Online Consumer Bill of Rights

Privacy online

Heuristic: where’s the disruption?

Employer health programs OK to share?

Data/metadata, w/Kift

Regulating IoT and mobile

CI + Ethics + Policy

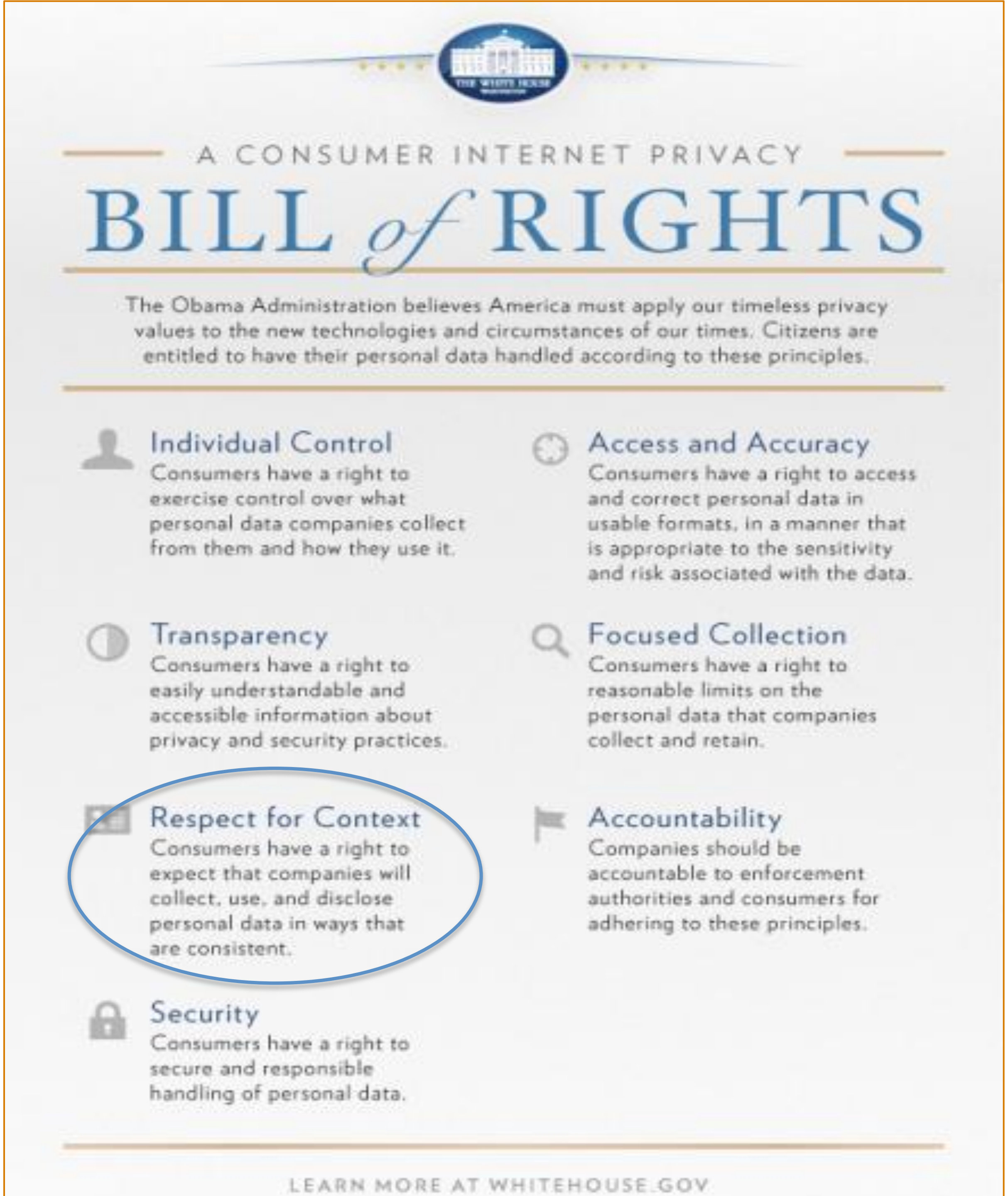
MOOCs + Education w/Zeide

Trouble with FIPPs

Practical obscurity made rigorous

Online court records, w/Conley, Datta, Sharma

Ethics of data mining: bias, privacy, autonomy



A CONSUMER INTERNET PRIVACY

BILL of RIGHTS

The Obama Administration believes America must apply our timeless privacy values to the new technologies and circumstances of our times. Citizens are entitled to have their personal data handled according to these principles.

Individual Control

Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

Access and Accuracy

Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity and risk associated with the data.

Transparency

Consumers have a right to easily understandable and accessible information about privacy and security practices.

Focused Collection

Consumers have a right to reasonable limits on the personal data that companies collect and retain.

Respect for Context

Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent.

Accountability

Companies should be accountable to enforcement authorities and consumers for adhering to these principles.

Security

Consumers have a right to secure and responsible handling of personal data.

LEARN MORE AT WHITEHOUSE.GOV

Feb 23, 2012

White House announces Privacy Bill of Rights

CI Ethics + Policy

White House Online Consumer Bill of Rights

Heuristic: where's the disruption?

Employer health programs OK to share?

Data/metadata, w/Kift

Regulating IoT and mobile

MOOCs + Education w/Zeide

~Open data

Trouble with FIPPs

Online court records, w/Conley, Datta, Sharma

Practical obscurity made rigorous

Privacy online

Ethics of data mining: bias, privacy, autonomy

Fitbit study, w/Patterson

Connecting privacy norms with contextual teleology (social and critical theory)

Sensitive information confounded, w/Martin

Evolution of norms in new mediated social spaces

Social science and theory

Interpersonal differences and commonalities

From where do contextual informational norms come?

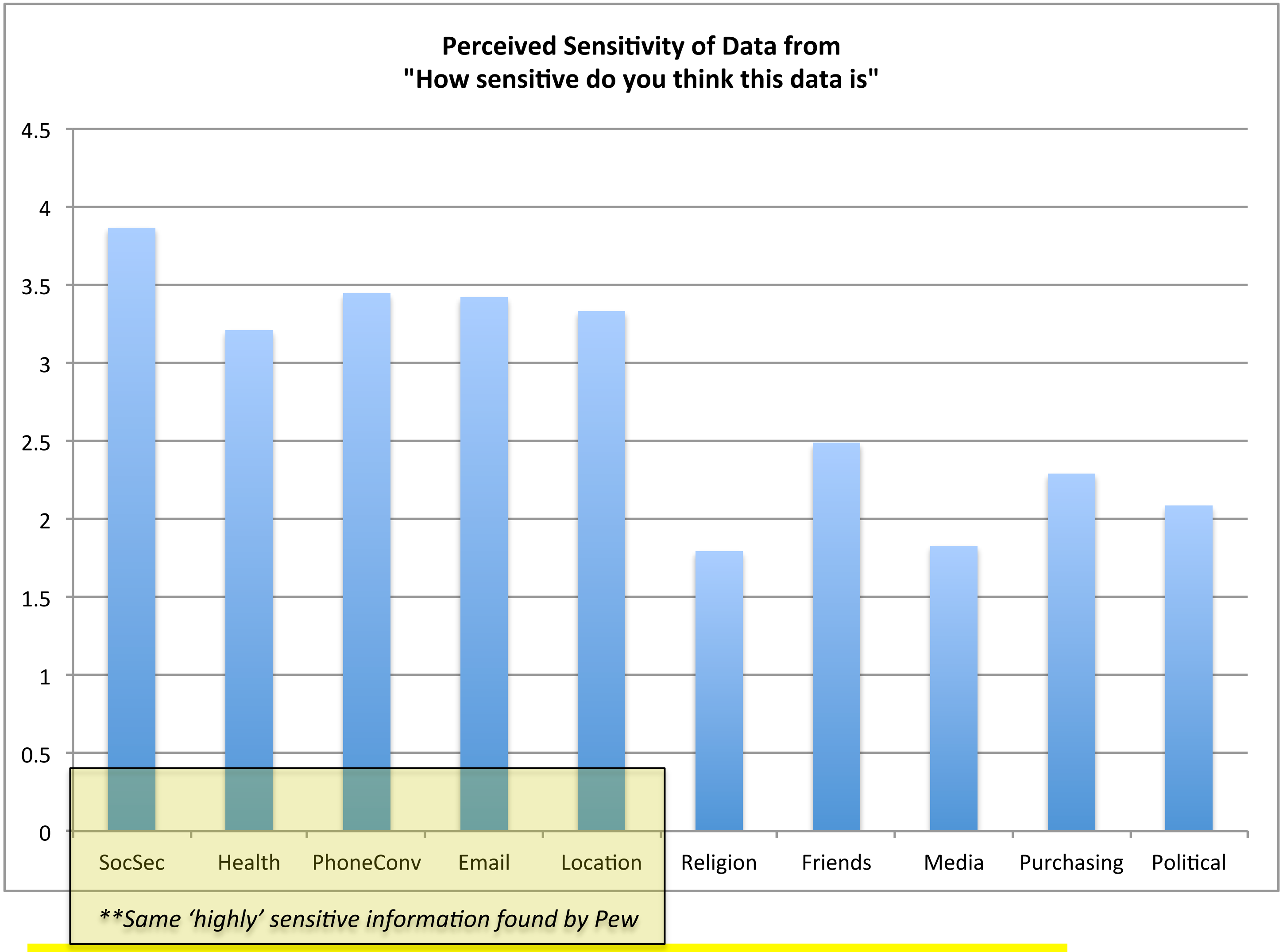
Methodologies for uncovering/discovering Contextual norms

Anthropological observer studies

Explaining cultural differences

“Confounding (contextual) variables” W/ K. Martin

Categories of Sensitive Information



***Same 'highly' sensitive information found by Pew*

ATTRIBUTES (taken from Pew Study language):

Religion: Your religious and spiritual views;
Friends: your friends and what they like;
Political: your political views and candidates you support;
Purchase: your purchasing habits;
Health: the state of your health and medications you take;
Location: details of your physical location over time.
Soc Sec: your social security number (new from pilot)

Context	
Retail	A clothing store
Employer	Your workplace
Education	Your school or university
Medical	Your doctor
Health	Your health insurance company
Search	An online search website
Library	Your local library

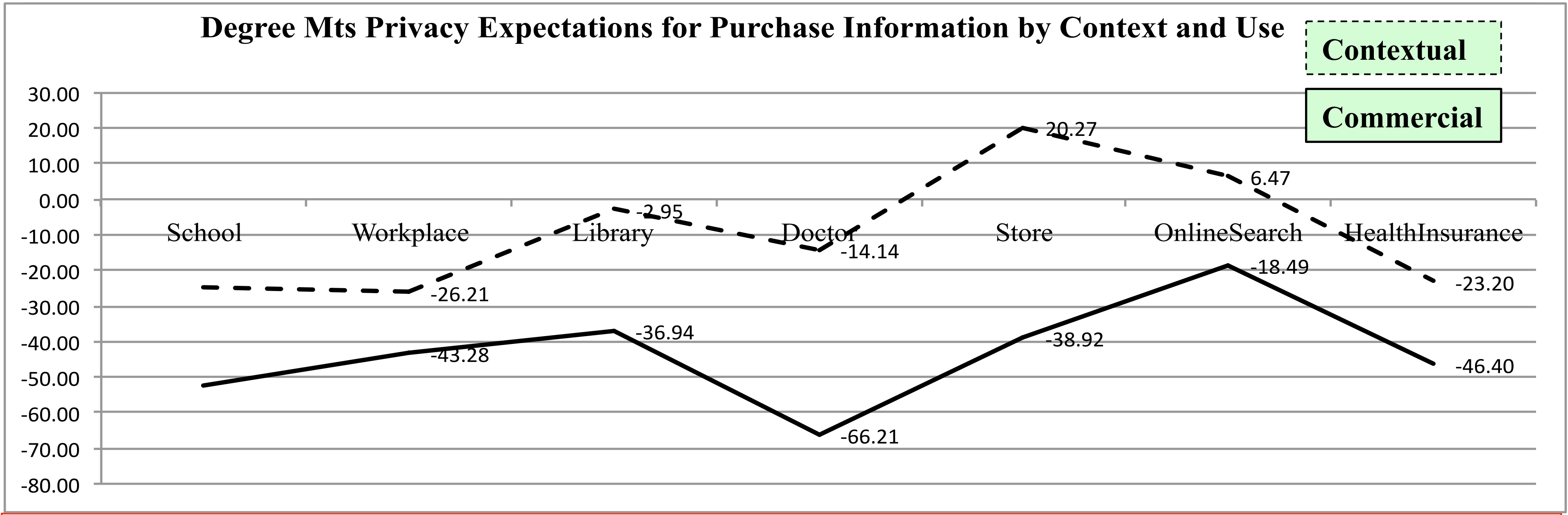
Vignette Design

Information about {Attributes} is collected by a {Contextual actor} for {Contextual or Non-Cntx'l use}.

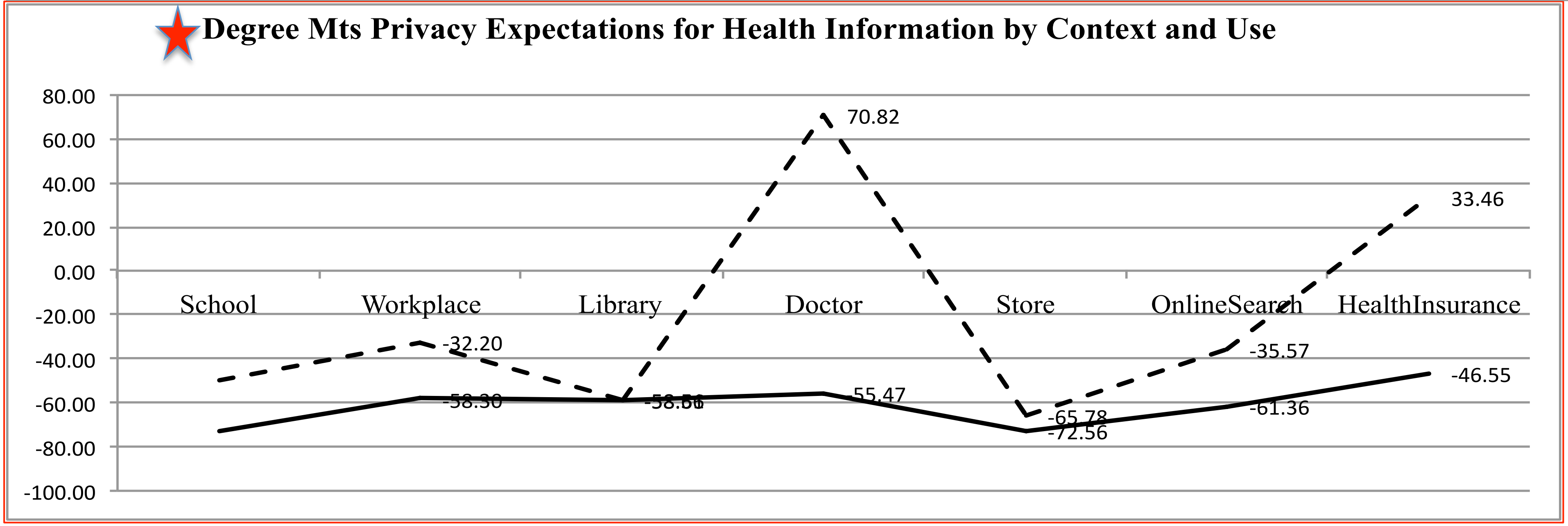
RATING: This meets my privacy expectations
Strongly Disagree … Strongly Agree

Context	Appropriate Flow	Non-Appropriate Flow
Retail	Make recommendations for you	sell to tracking company who combines the data with your other activities
Employer	Identify employee programs you might be interested in	Offer to outside companies to market products and services to you;
Education	Place students in groups for class	Offer to financial companies to market credit cards and loans to students;
Medical	To diagnose and treat your condition	To sell to pharmaceutical companies for marketing and advertising
Health	To detect fraud	Sell to drug stores for marketing;
Search	Prioritize search results	Place tailored ads when you are on other sites.
Library	To make book recommendations for you	To notify other organizations of your preferences for fundraising or sales.

Purchasing and Health Information Confounded



Degree Mts Privacy Expectations for Purchase Information by Context and Use

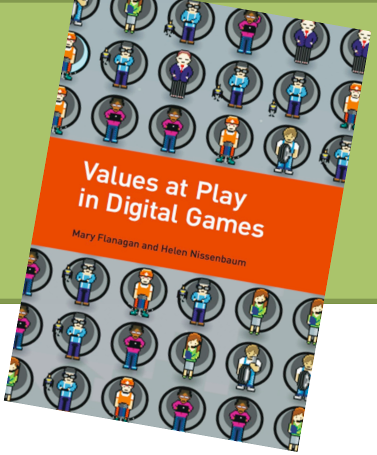


Degree Mts Privacy Expectations for Health Information by Context and Use

Privacy by design

Science & Engineering

Values @ Play



DISCOVERY

I. What values? Sources?

II. Define in operational terms

IMPLEMENTATION

I. Translate values into features and architecture

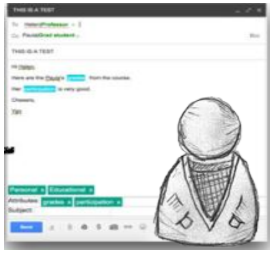
II. Resolve conflicts: dissolve, compromise, tradeoff

VERIFICATION

Action/outcome, understanding, affect/attitude

Prototype, user studies, reflection

VACCINE: For building privacy aware information systems



THIS IS A TEST

To Helen/Professor

Cc Paula/Grad student

Bcc

THIS IS A TEST

Hi Helen,

Here are the Paula's grades from the course.

Her participation is very good.

Cheers,

Yan

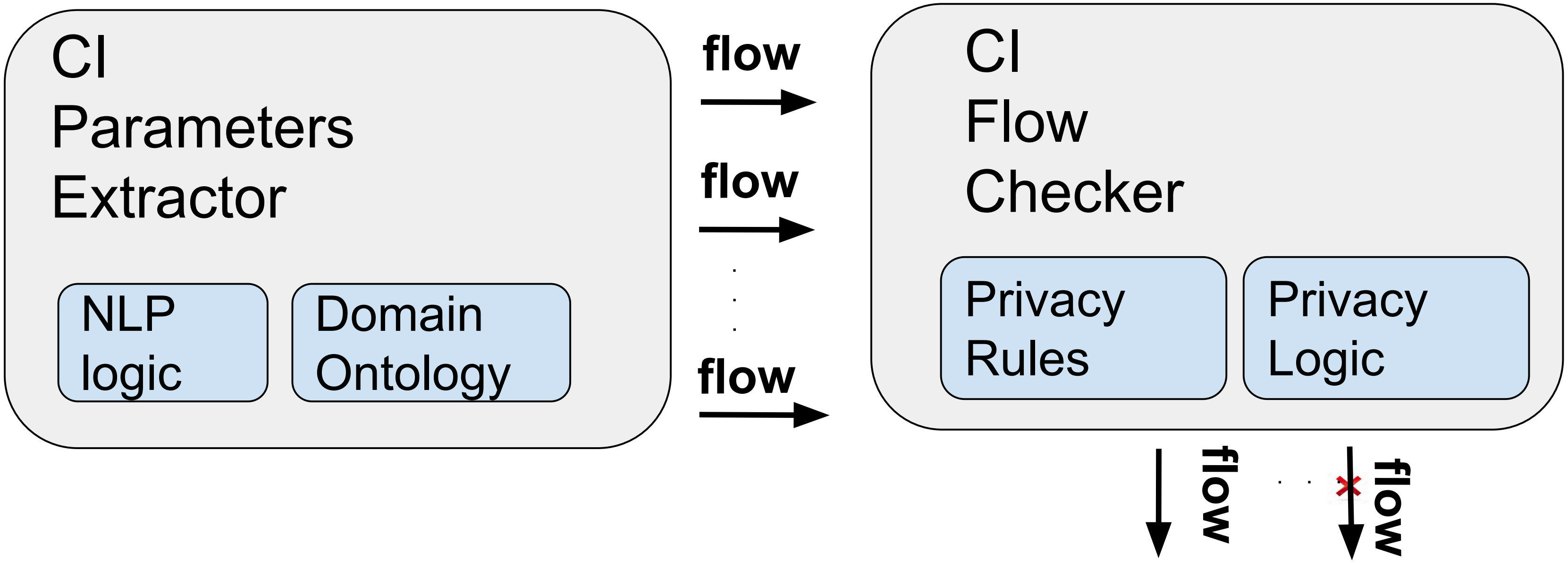
Attributes: grades × participation ×

Subject:

VACCINE: **V**erifiable & **AC**tionable **C**ontextual **I**ntegrity **N**orms **E**ngine

Message Metadata

CONTENT



THIS IS A TEST

To Helen/Professor

Cc Paula/Grad student

THIS IS A TEST

Hi Helen,

Here are the Paula's grades from the course.

Her participation is very good.

Cheers,

Yan

Personal × Educational ×

Attributes: grades × participation ×

Subject:

Send

Y. Shvartzshnaider, P. Kift, T. Wies, Z. Pavlinovic,
H. Nissenbaum, S. Tong, L. Subramanian, P. Mittal

Mturk Study
Sample questions and answers

- Final question format:

Is it acceptable for the <sender> to share the <subject>'s <attribute> with <recipient> <transmission principle>?

- Answers:

1) Yes
2) No
3) Does not make sense (DMS)
   a) The sender is unlikely to have the information
   b) The receiver would already have the information
   c) The question is ambiguous

- Example 1: Is it acceptable for the registrar to share the student's name with graduate schools if the registrar asked for the student's permission?

1) Yes (85%)
2) No (9%)
3) Does not make sense (DMS)
   a) The sender is unlikely to have the information (0%)
   b) The receiver would already have the information (6%)
   c) The question is ambiguous (0%)

Sample questions and answers

- Example 2: Is it acceptable for the student's TA to share the student's email address with the student's academic advisor if requested by the student's academic advisor?

1) Yes (37%)
2) No (30%)
3) Does not make sense (DMS)
   a) The sender is unlikely to have the information (9%)
   b) The receiver would already have the information (24%)
   c) The question is ambiguous (0%)

- Example 3: Is it acceptable for the student's professor to share the student's transcript with the student's academic advisor if the student's professor asked for the student's permission?

1) Yes (63%)
2) No (6%)
3) Does not make sense (DMS)
   a) The sender is unlikely to have the information (9%)
   b) The receiver would already have the information (22%)
   c) The question is ambiguous (0%)

Obfuscation

TrackMeNot+Adnauseam

Learn norms using ML

ID contexts using NLP

VACCINE

Privacy by design

“Small data”- IoT Flows w/Estrin

Science & Engineering

Formal expression of flow/access rules

Handoff Tech <-> Law/policy w/Mulligan

CI concepts to tech properties
Actors (roles, ..)
Info types (tag, watermark, …)
TPs (authorize,)

Technique, system, architecture, model, algorithm, mechanism, scenario, protocol

On the horizon …

© www.backgroundpictures.org

Future directions

- **Make CI more usable for science, engineering, & design**
- **We NEED the equivalent of privacy threat models!**
- **Empirical and historical studies to source and locate informational norms**
- **Further work to understand links between information flows, and contextual purposes and values they serve.**
- **Confronting challenges of big data, data mining, and machine learning to CI?!**
- **Overcoming challenges to CI (too many moving parts) utilizing big data and machine learning**