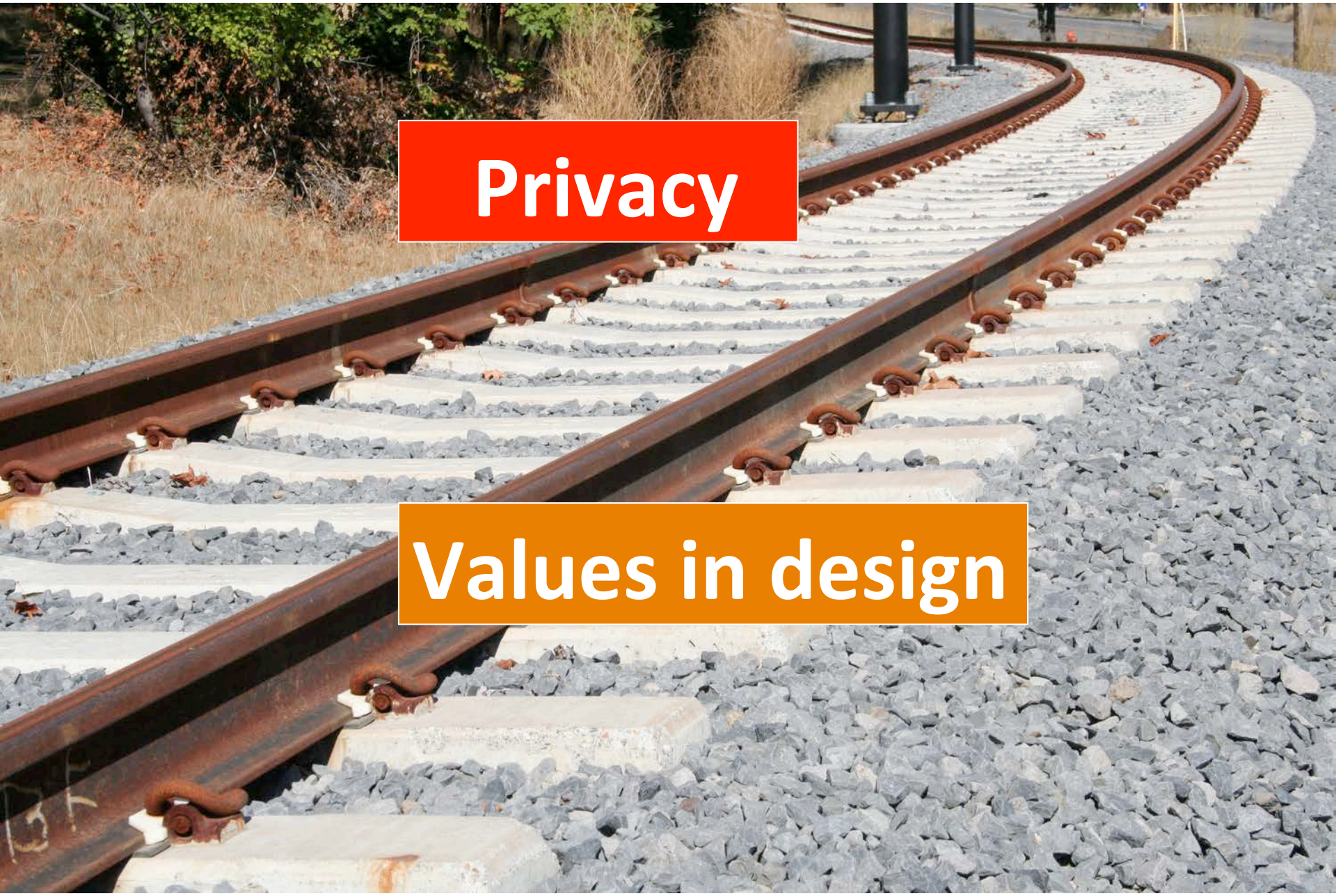
At the Intersection of Ethics and Technology: Contextual Integrity and other Values

Helen Nissenbaum
New York University

Interdisciplinary Summerschool on Privacy
July 2016 Hotel Erika, Berg en Dal


Privacy
Values in design

Outline

- Values in Design – Values at Play
- Contextual Integrity Fundamentals
- Applications and Testing: regulation, social sciences, technology


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

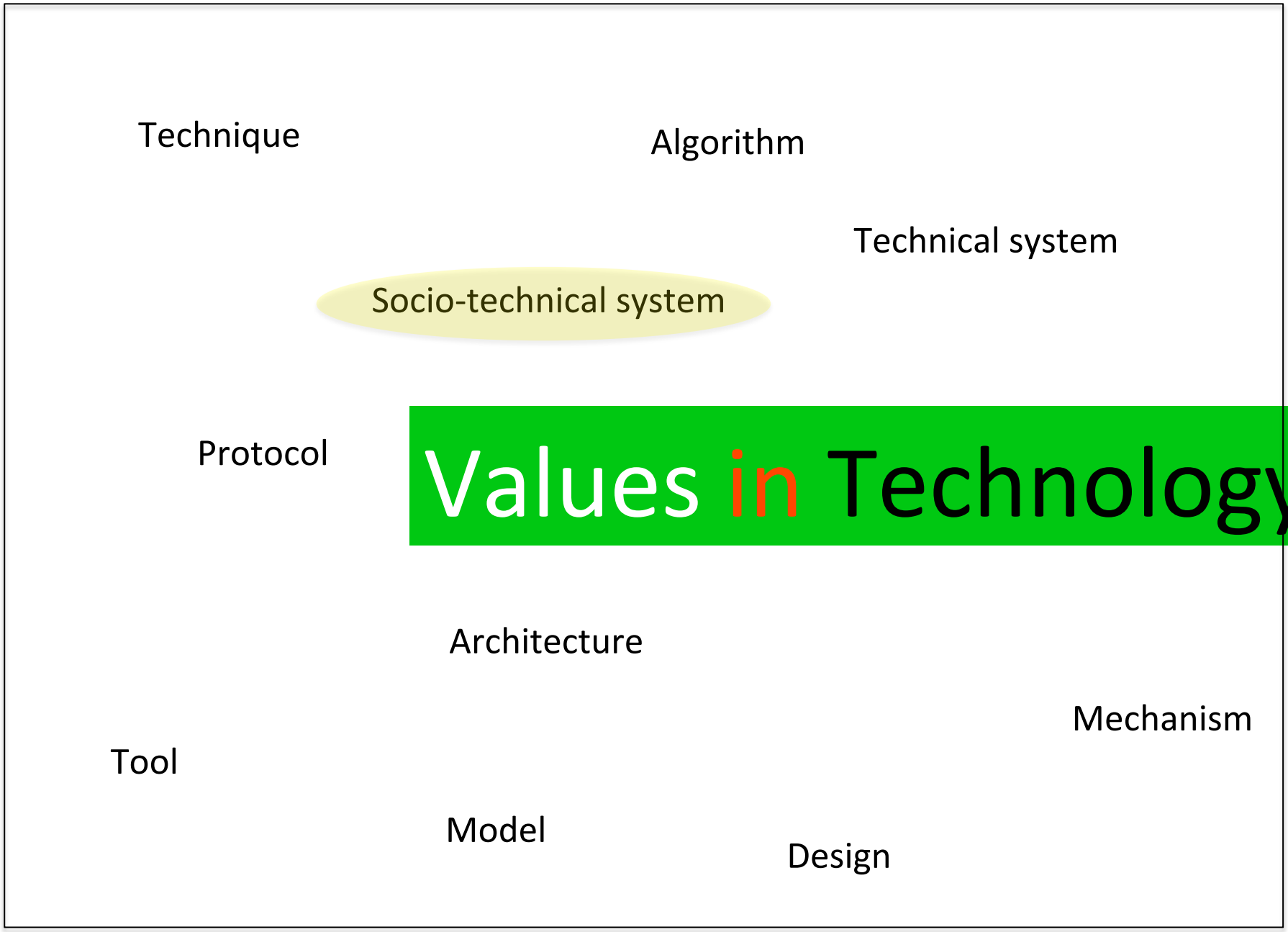
Values in Design

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

Values in technology are not simply a function of use but of design

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

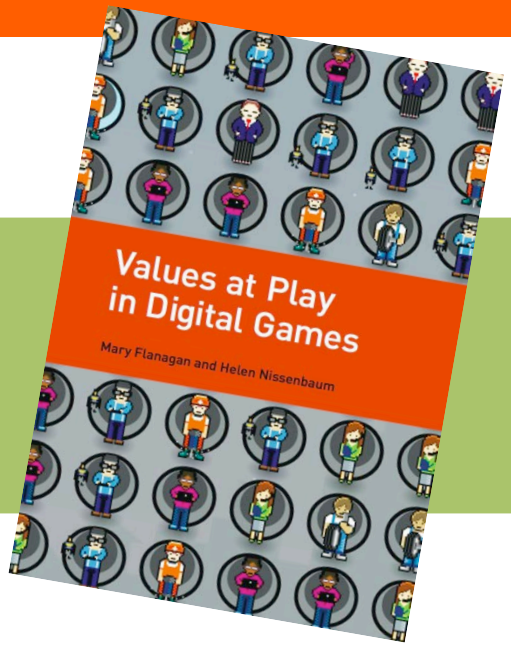
The belief that technical properties and ethical (political) properties can be “lined up” in certain ways

The “practical turn”: design *for* values

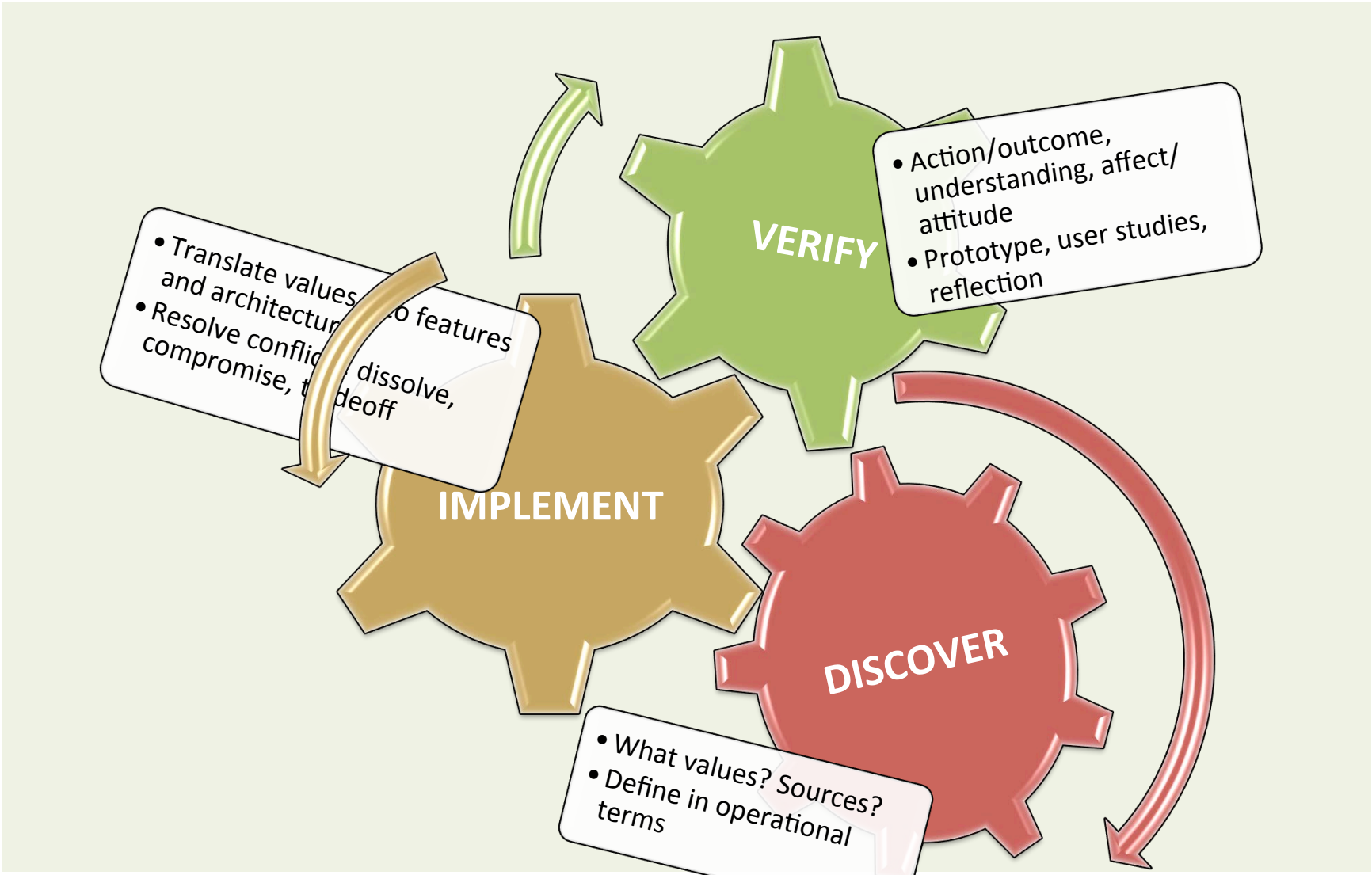
THE PRACTICAL TURN …

Values @ Play

Howe, Flanagan, Nissenbaum

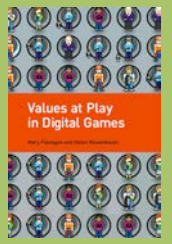


Values @ Play


VERIFY
• Action/outcome, understanding, affect/ attitude
• Prototype, user studies, reflection
IMPLEMENT
• Translate values
and architectur
• Resolve conflic
compromise, t
o features
dissolve,
deoff
DISCOVER
• What values? Sources?
• Define in operational terms

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


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)

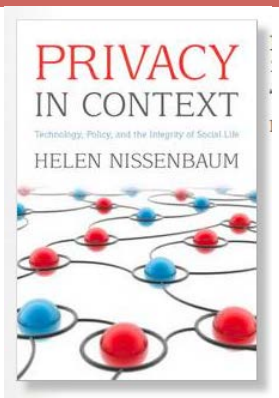
“privacy in public” (1997)

CONCEPTUAL PUZZLE

SOLUTION 2004

Theory of Contextual Integrity

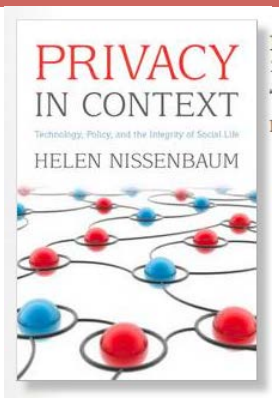
Contextual Integrity Fundamentals



In hindsight:

4 essential claims

Contextual Integrity Fundamentals



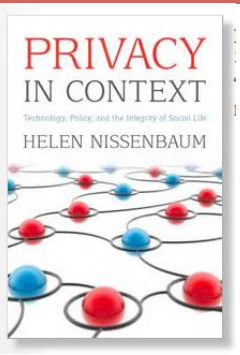
I. Privacy as <u>appropriate</u> <u>flow</u>

NOT

Information leakage = privacy violation (Alice, Bob, Eve)
Any collection = privacy violation

"No-flow"/secrecy = privacy

Contextual Integrity Fundamentals



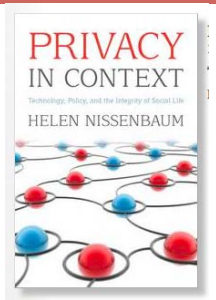
II. Appropriate flow as conformance with contextual informational norms (= "contextual integrity")

NOT

The upshot of procedure, e.g.

- FIPPs
- Informed consent
- … etc.

Contextual Integrity Fundamentals



III. Contextual informational {privacy} norms include five independent, parameters: <subject, sender, recipient>, <information type>, <transmission principle>

NOT

Subject control

Public/Private/Sensitive

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

sender subject Information type

Equifax provides Daisy White's credit report to

Wells Fargo Bank with authorization from Daisy White

recipient Transmission principle

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

Informational Norm for Context C

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

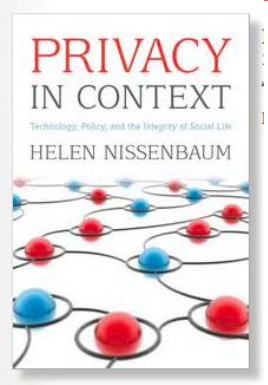
$$\text{incontext}(p_1, c) \wedge \text{send}(p_1, p_2, m) \wedge \text{contains}(m, q, t) \rightarrow \bigvee_{\varphi^+ \in \text{norms}^+(c)} \varphi^+ \wedge \bigwedge_{\varphi^- \in \text{norms}^-(c)} \varphi^-$$

positive norm: $\text{inrole}(p_1, \hat{r}_1) \wedge \text{inrole}(p_2, \hat{r}_2) \wedge \text{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \wedge \psi$

negative norm: $\text{inrole}(p_1, \hat{r}_1) \wedge \text{inrole}(p_2, \hat{r}_2) \wedge \text{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \rightarrow \psi$

BARTH, A., A. DATTA, J.C. MITCHELL, AND H. NISSENBAUM, Privacy and contextual integrity: Framework and applications. In *Proc. of IEEE Symposium on Security and Privacy 2006*.

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 …

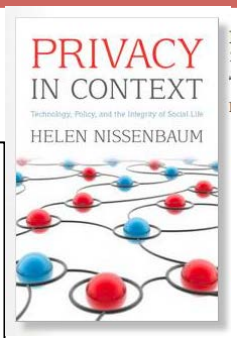
education: knowledge, intellect, fair distribution

"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

Data/Metadata (+Paula Kift)
Forthcoming in I/S Law and Policy Journal

CI + Ethics + Policy

Online court records, w/Conley, Datta, Sharma

Open data

Trouble with FIPPs

DLPs and Education w/Zeide

Feb 23, 2012

White House announces Privacy Bill of Rights

White House Online Consumer Bill of Rights

Privacy online

Data/Metadata (+Paula Kift)
Forthcoming in I/S Law and Policy Journal

CI + Ethics + Policy

Online court records, w/Conley, Datta, Sharma

Open data

Trouble with FIPPs

DLPs and Education w/Zeide

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

Revisiting & debunking "classic" privacy surveys (+Kirsten Martin)

Connecting privacy norms with contextual purpose

Evolution of norms in new mediated social spaces

IoT/Fitbit study, (+HeatherPatterson

Social science and theory

Interpersonal differences and commonalities

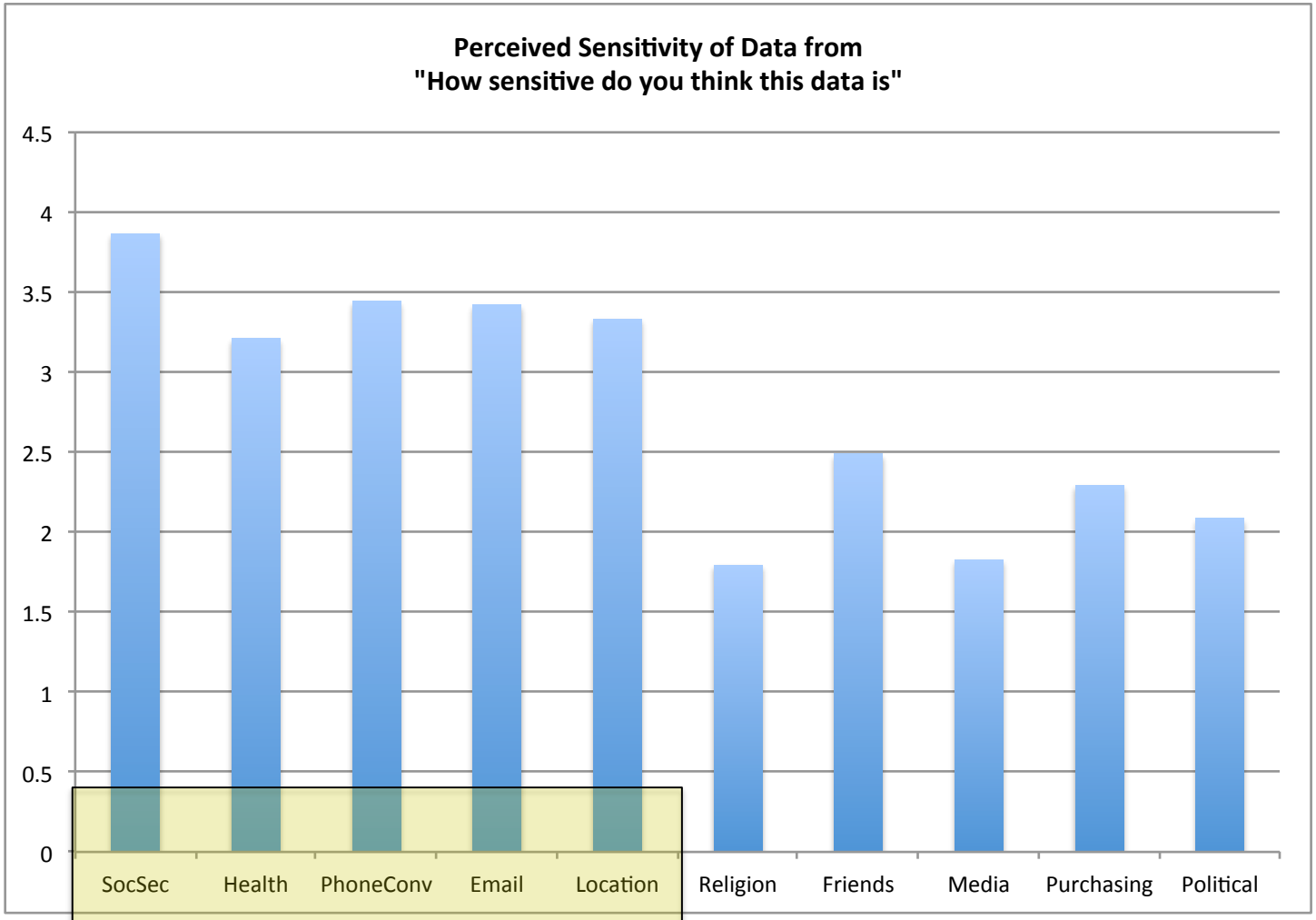
Origins of contextual informational norms

Methods for discovering Contextual norms

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)

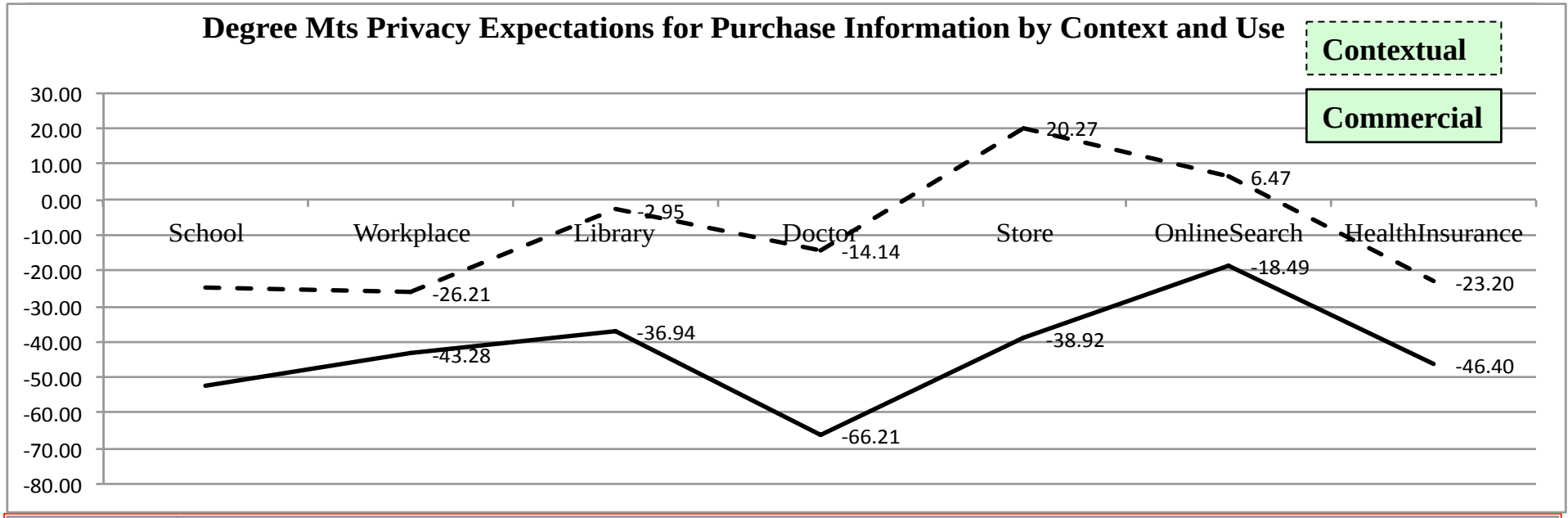
Context	
Retail	A clothing store
Employer	Your workplace
Education	Your school or university
Medical	Your doctor
Health	Your health insurance company
Search	An online search website
Library	Your local library

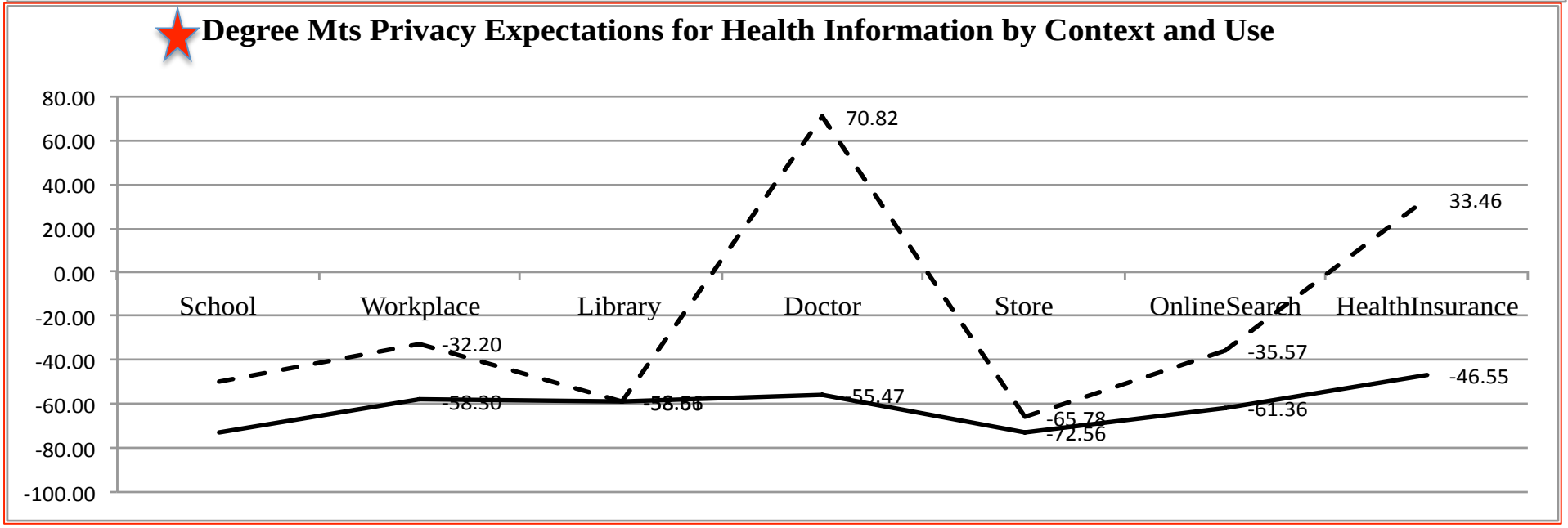
Information about {Attributes} is collected by a {Contextual actor} for {Contextual or Non-Cntx'l use}.

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





Privacy by design

Science & Engineering

Obfuscation

TrackMeNot. Adnauseam

Formal expression of flow/access rules

"Small data"- IoT Flows w/Estrin

Science & Engineering

CI Norms for social platforms

Privacy by design

NLP to ID Contexts

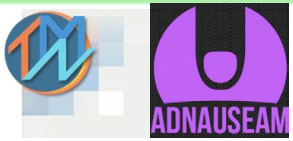
Technique, system, architecture, model, algorithm, mechanism, scenario, protocol

Actionable CI for Privacy Engineering w/Seda Guerses

Handoff Tech <-> Law/policy w/Mulligan

Obfuscation

TrackMeNot+Adnauseam



Learning privacy norms using ML

ID contexts using NLP

"Small data"- IoT Flows w/Deborah Estrin

Privacy by design

Science & Engineering

Formal expression of flow/access rules

Actionable CI for Privacy Engineering w/Seda Guerses

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

Handoff Tech <-> Law/policy w/Deirdre Mulligan