

Values in Design & Contextual Integrity

Helen Nissenbaum

Politics in technology: call to action

Langdon Winner

“Do Artifacts have Politics?” In *The Whale and the Reactor* 1988

“In that sense technological innovations are similar to legislative acts of political foundings that establish a framework for public order that will endure over many generations. ... The issues that divide or unite people in society are settled not only in the institutions and practices of politics proper, but also, and less obviously, in tangible arrangements of steel and concrete, wires and semiconductors, nuts and bolts.” (p.29)

[[... and we may add, “lines of code.”]]

(others) Technical things embody moral and political values

“Democratic & authoritarian technics”

Lewis Mumford, 1964

“The medium is the message”

Marshall McLuhan, 1964

“Invisible values embedded in computer programs,”

James Moor, 1985

“The missing masses”

Bruno Latour, 1992

“STS ... the political philosophy of our time”

Brian Pfaffenberger, 1992

“Code as law”

Lawrence Lessig, 1999

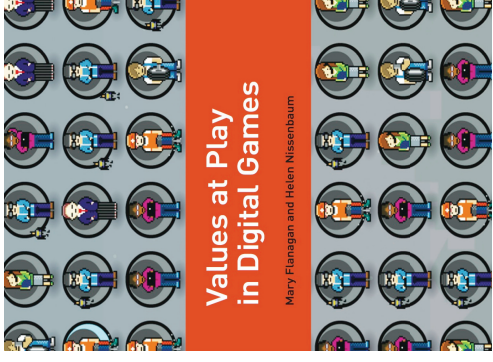
Not (only) implications after the fact

From analysis to practice

The practical turn:
taking values into consideration in the
practice of design and development

VID in FIA

How?



Values at Play



Value sensitive design



Values @ Play

[Howe, Flanagan, Nissenbaum]



DISCOVER

What values? Sources?

Define in operational terms

IMPLEMENT

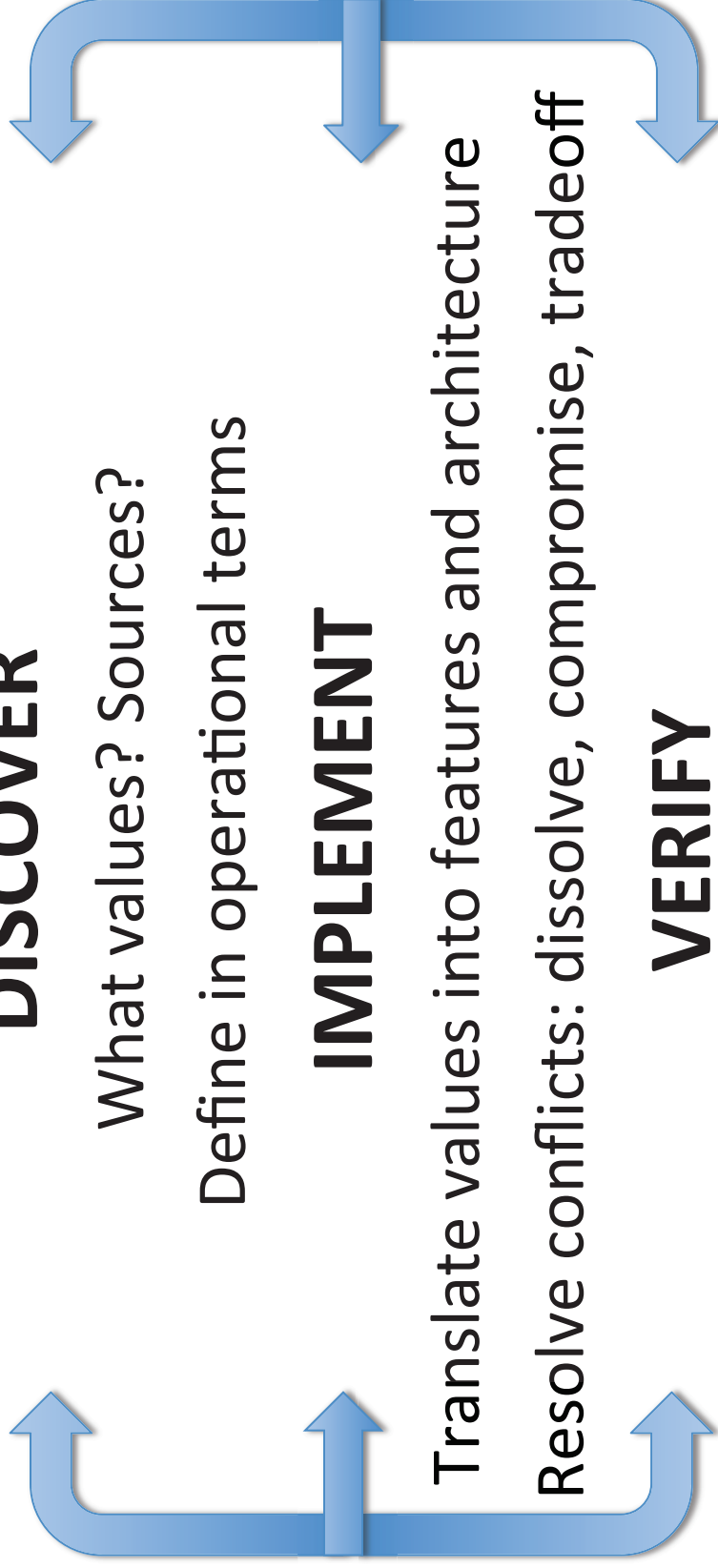
Translate values into features and architecture

Resolve conflicts: dissolve, compromise, tradeoff

VERIFY

Action/outcome, understanding, affect/attitude

Prototype, user studies, reflection



Values @ Play

DISCOVERY I: What values? Sources?

Functional description: Secure transmission

Collateral: toaster, email, web-cookies

Key Actors: designers, builders, funders, users

Societal context: culture, **tech standards**, board ratings ..

Technical/material constraints: screen size



Values @ Play

DISCOVERY II: Define abstract concepts operationally

Social justice: gender equity, equal access to good jobs

Openness: decentralized access, free-for-all, protocol, free of charge

Loyalty: favoritism, affirmative action for friends and family

Bias: systematic unfairness

...

Privacy: control, secrecy, contextual integrity,
multi-dimensional analytic

Values @ Play

IMPLEMENTATION = Translate values

Architecture, mechanism, protocol, algorithms, rules

In order to

Force, constrain, prevent, impede, instruct,

“Nudge,” afford, allow

Configure, cost, convention, know-how

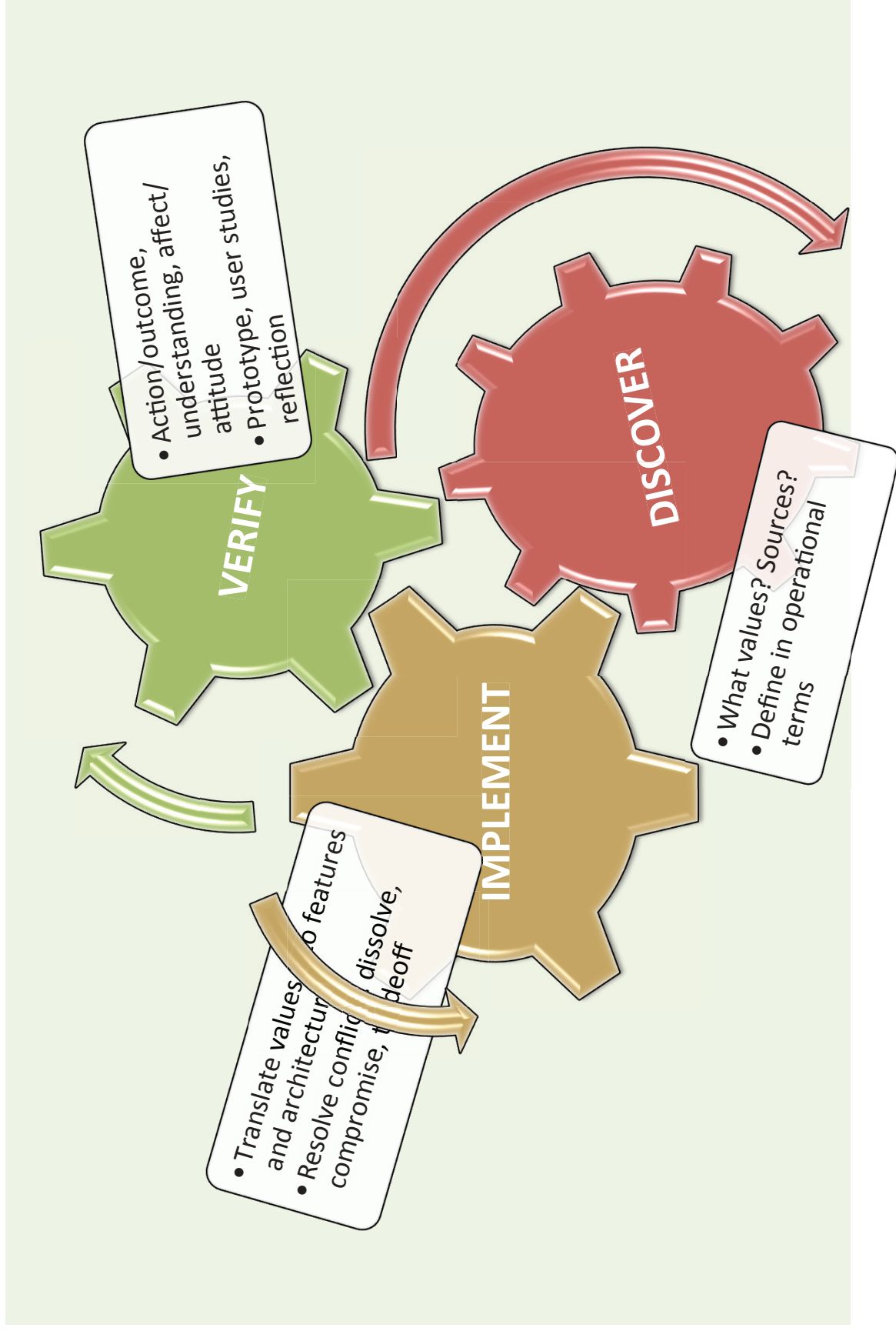
Resolve conflicts

Dissolve

Compromise

Tradeoff

Values @ Play

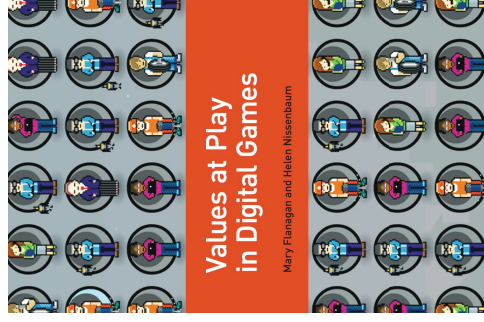




Giant (10ft) Joystick Mary Flanagan



“at play”





A Theory of Privacy as Contextual Integrity



1 Privacy means appropriate information flow
(Not control, secrecy, or dichotomy)

2 Appropriateness means compliance with
social expectations of privacy

3 Expectations of privacy are modeled by
Context specific informational norms

4 Ideal informational norms are those that
promote ethical and political principles
and contextual ends, purposes, and values

Underlying Assumptions of Privacy as CI

Contexts

Structured social spheres defined by activities, practices, roles, ... e.g. healthcare, education, social & home-life, professional & work-life, commercial marketplace

Informational Norms

Context specific rules, customs, conventions, expectations, laws, defining appropriate flows of personal information

Purposes and values

Ends, purposes, values in a context, both specific and general

Informational norms model expectations

In a job interview, the interviewer asks about a candidate's past work experience but not about religious observance

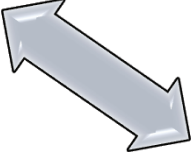
A priest never shares congregants' confessions with others

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

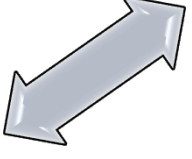
You do not share a friend's secrets with others, except, perhaps, with your spouse, unless your friend expressly requests otherwise

Parents closely monitor their children's academic performance

Theory of Contextual Integrity



Structure of
Informational norms



Capturing the value
of privacy

Informational norms: Structure

Actors

Sender
Recipient
Subject

Physician, merchant, bank, friend
Merchant, police, ad network
Patient, shopper, investor, reader

Information types

Demographic, biographical
Transactional, communications
Medical status, financial

Transmission Principles

Consent, coerce, steal, buy, sell
Confidentially, stewardship
With a warrant, surreptitiously
[An indefinitely large domain]

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

^{Sender} Equifax provides ^{Subject} Daisy White's ^{Information type} credit report to ^{Recipient} Wells Fargo Bank with authorization from Daisy White
Transmission principle

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

Informational Norms Embedded in Law: Example (GLB Act)

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,

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

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

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

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

Kirsten Martin, “An empirical study of factors driving privacy expectations online.” (PLSC 2013)

50% of respondents believed targeting vignettes did not conform to the privacy notice

70% of respondents believed tracking vignettes did not conform to the privacy notice to some degree.

... *when they did!*

Those who said vignettes conformed to privacy notice were only somewhat certain

In our case studies: Policy vs. normative expectations

+ Tesla Tussle

+ Warning of the presences of licence plate readers

PbD Takeaways

Establish context
Map flow to/from
ALL actors
Information types
Transmission principles

All the parameters matter!!
Omission invites ambiguity

PbD Takeaways

- Design principles (per Rubinstein)
- Data minimization
- Enforce flow patterns
- Implement constraints (e.g. crypto)
- Authorization and authentication

But: What makes this about PRIVACY?
Not, e.g. security, or DRM, ...?

Capturing the Value of Privacy with CI, or *why we should care about informational norms*

- Interests
- General moral, social, and political values
- Internal context-specific ends, purposes and values

What counts in the privacy calculus?

Interests – often conflicted

Informational harms, benefits, risks

Boundary control (Altman)

General moral, social, and political rights & values

Unfair discrimination ...

Liberty, autonomy ...

What counts in the CI calculus

Context specific 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

PbD Takeaways

The harm calculus
About individuals data subjects
and
Social integrity

Contextual ends, purposes, & values