Implications of Context for Regulation

Jesse Sowell

Engineering Systems Division, MIT
Advanced Network Architecture Group, CSAIL

Overview

- Two distinct privacy regulatory paradigms:
  - **EU**: socially protective
  - **US**: normatively liberal
- **Problem:** Tools available to these two privacy paradigms may not efficiently map to privacy paradigms rooted in a context metaphor
- **Illustrative Instance:** Surfacing the privacy implications of behavioral advertising in information rich contexts
  - Cyber environments
  - Cyber+terrestrial via mobile platforms
  - Smart power grid
- **Question:** How do we create sufficiently responsive standards development processes?
  - What are the roles of regulatory bodies?
  - What might a hybrid regime look like?
  - What are the politically and strategically feasible incentive structures for developing supporting metrics?

Overview

- Two distinct privacy regulatory paradigms:
  - **EU**: socially protective
  - **US**: normatively liberal
- **Problem:** Tools available to these two privacy paradigms may not efficiently map to privacy paradigms rooted in a context metaphor
- **Illustrative Instance:** Surfacing the privacy implications of behavioral advertising in information rich contexts
  - **Cyber environments**
  - Cyber+terrestrial via mobile platforms
  - Smart power grid
- **Question:** How do we create sufficiently responsive standards development processes?
  - What are the roles of regulatory bodies?
  - What might a hybrid regime look like?
  - What are the politically and strategically feasible incentive structures for developing supporting metrics?

Regulation and Fair Information Practices (FIPs) Origins

Regulation and Fair Information Practices (FIPs) Origins

- Modern regulation rooted in the FIPs

Regulation and Fair Information Practices (FIPs) Origins

- Modern regulation rooted in the FIPs
- Evolved in the privacy climate of the 60's and 70's

Regulation and Fair Information Practices (FIPs) Origins

- Modern regulation rooted in the FIPs
- Evolved in the privacy climate of the 60's and 70's
- Response to government use of mainframes

Regulation and Fair Information Practices (FIPs) Origins

- Modern regulation rooted in the FIPs
- Evolved in the privacy climate of the 60's and 70's
- Response to government use of mainframes
- Concurrently developed in US and EU
  - Younger Committee (UK, early 1970's)
  - Westin and Baker's recommendations to National Academies (1972)
  - Nascent articulations in 1970 Fair Credit Reporting Act
  - 1974 Privacy Act
  - COE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)
  - OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data

Regulation and Fair Information Practices (FIPs) Origins

- Modern regulation rooted in the FIPs
- Evolved in the privacy climate of the 60's and 70's
- Response to government use of mainframes
- Concurrently developed in US and EU
  - Younger Committee (UK, early 1970's)
  - Westin and Baker's recommendations to National Academies (1972)
  - Nascent articulations in 1970 Fair Credit Reporting Act
  - 1974 Privacy Act
  - **COE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)**
  - **OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data**

FIPs as Guidelines

- **Openness:** repository known data subjects
- **Access and Correction:** ability to ensure accuracy
- **Collection Limitation:** collected fairly with consent of data subject
- **Use Limitation:** limited to original uses; *relevance*
- **Disclosure Limitation:** data may not be shared with without consent of subject
- **Security Principle:** sufficient safeguards

FIPs as Guidelines

- **Openness:** repository known data subjects
- **Access and Correction:** ability to ensure accuracy
- **Collection Limitation:** collected fairly with consent of data subject
- **Use Limitation:** limited to original uses; *relevance*
- **Disclosure Limitation:** data may not be shared with without consent of subject
- **Security Principle:** sufficient safeguards

1. Control metaphor
   - Notice mechanisms
   - Opt-in/opt-out

FIPs as Guidelines

- **Openness:** repository known data subjects
- **Access and Correction:** ability to ensure accuracy
- **Collection Limitation:** collected fairly with consent of data subject
- **Use Limitation:** limited to original uses; *relevance*
- **Disclosure Limitation:** data may not be shared with without consent of subject
- **Security Principle:** sufficient safeguards

1. Control metaphor
   - Notice mechanisms
   - Opt-in/opt-out
2. Normative
   - Policy convergence and commonality
   - Need operationalization to become standards

FIPs as Guidelines

- **Openness:** repository known data subjects
- **Access and Correction:** ability to ensure accuracy
- **Collection Limitation:** collected fairly with consent of data subject
- **Use Limitation:** limited to original uses; *relevance*
- **Disclosure Limitation:** data may not be shared with without consent of subject
- **Security Principle:** sufficient safeguards

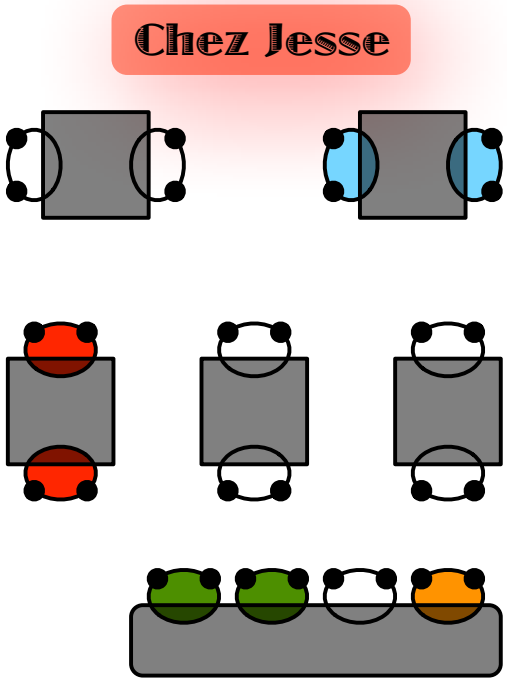
1. Control metaphor
   - Notice mechanisms
   - Opt-in/opt-out
2. Normative
   - Policy convergence and commonality
   - Need operationalization to become standards
3. What constitutes “personal” is ambiguous
   - Conventional PII captured
   - Aggregate image of attributes . . . ?

FIPs Implementation

- EU
  - Socially protective → privacy is an *inalienable* human right
  - Comprehensive regulation covers public and private sector
  - DPAs implement monitoring, audit, and enforcement
  - Top down comprehensive
  - Failure mode:
    - DPA capacity issues
    - DPA-company communication
- US
  - Normatively liberal → privacy is an *alienable* commodity that may be exchanged for utility
  - Ad hoc, sectoral, chaotic self-regulatory structure
  - Self-help: harms are identified as they emerge
  - Bottom up self-regulatory
  - Failure mode:
    - Information asymmetries
    - Collective action problems
- **Implications of Context?**

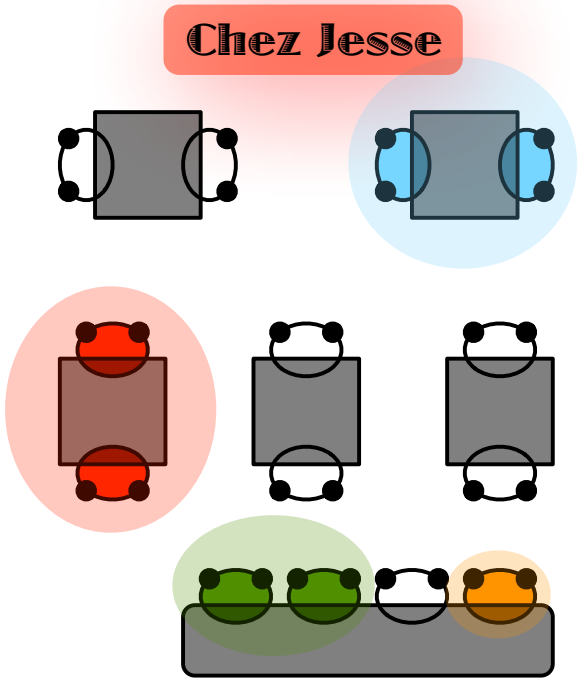
Context and Environment

- Environment is the “place”
  - Can be anywhere
  - Online: environment is architected
- Context is a social construction that occurs across environments
  - Rules of appropriateness
  - Rules of distribution



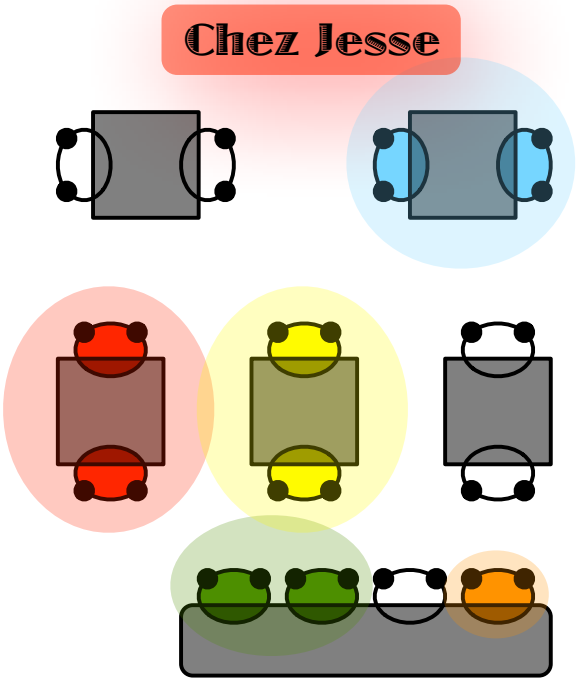
Context and Environment

- Environment is the “place”
  - Can be anywhere
  - Online: environment is architected
- Context is a social construction that occurs across environments
  - Rules of appropriateness
  - Rules of distribution
- Public place, still a notion of privacy



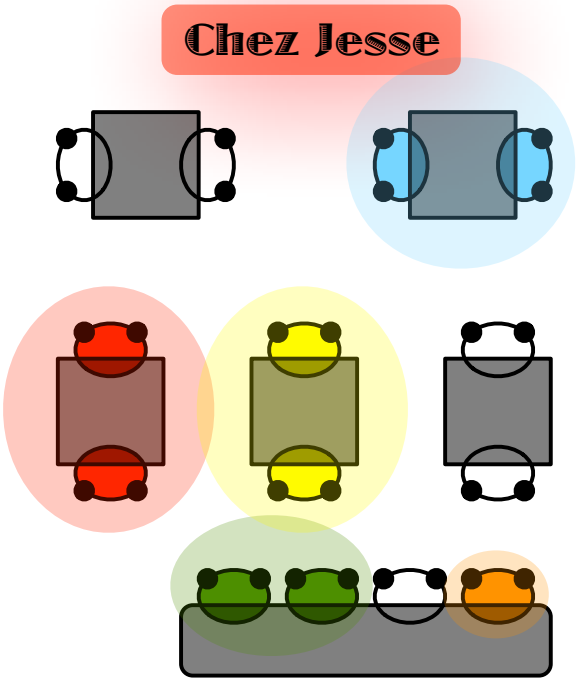
Context and Environment

- Environment is the “place”
  - Can be anywhere
  - Online: environment is architected
- Context is a social construction that occurs across environments
  - Rules of appropriateness
  - Rules of distribution
- Public place, still a notion of privacy
- Context changes when new actors enter



Context and Environment

- Environment is the “place”
  - Can be anywhere
  - Online: environment is architected
- Context is a social construction that occurs across environments
  - Rules of appropriateness
  - Rules of distribution
- Public place, still a notion of privacy
- Context changes when new actors enter

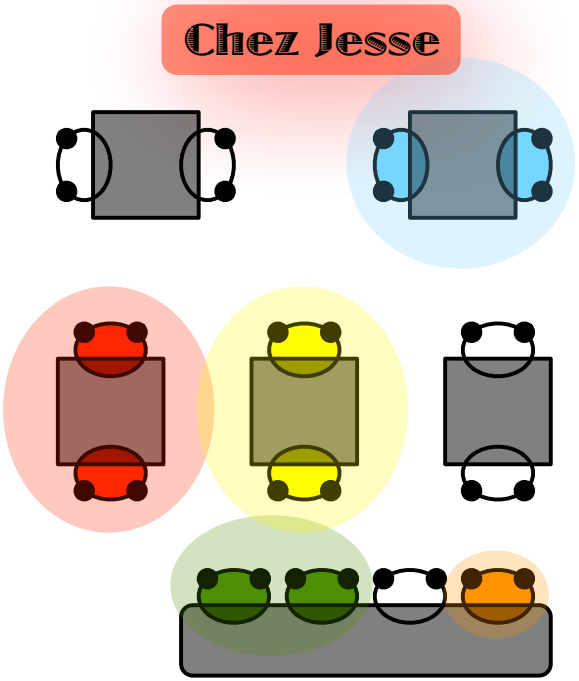


Trust and Visibility

Contextual integrity is based on trust amongst actors in a context and understanding the dynamics of the environment

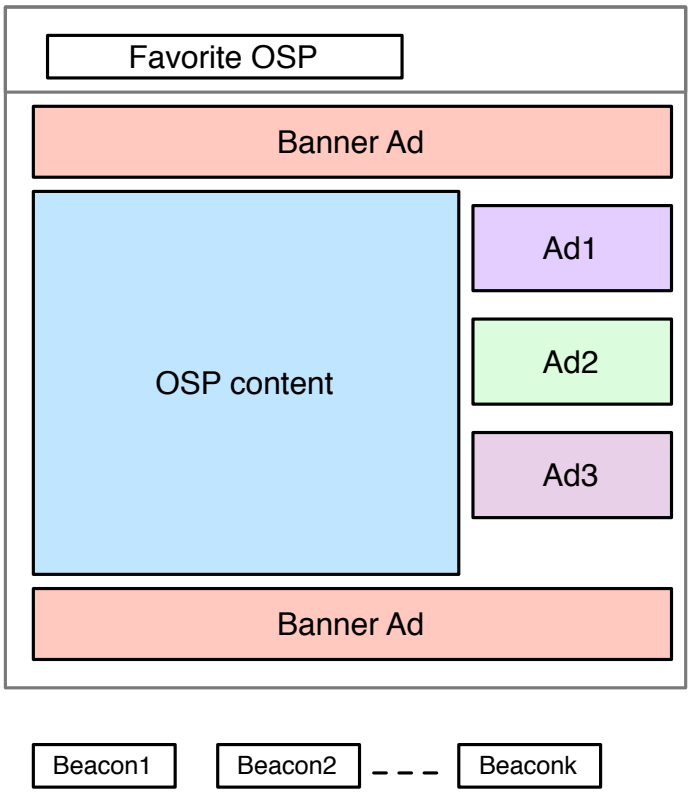
Tractability of Mixed Context

- Architectural dynamics defies establishing a trust relationship
  - Context different on each visit
  - Different actors “at the table”
- Lack of policy transitivity
  - OSP policy rooted in limiting liability
  - Contractual info absent



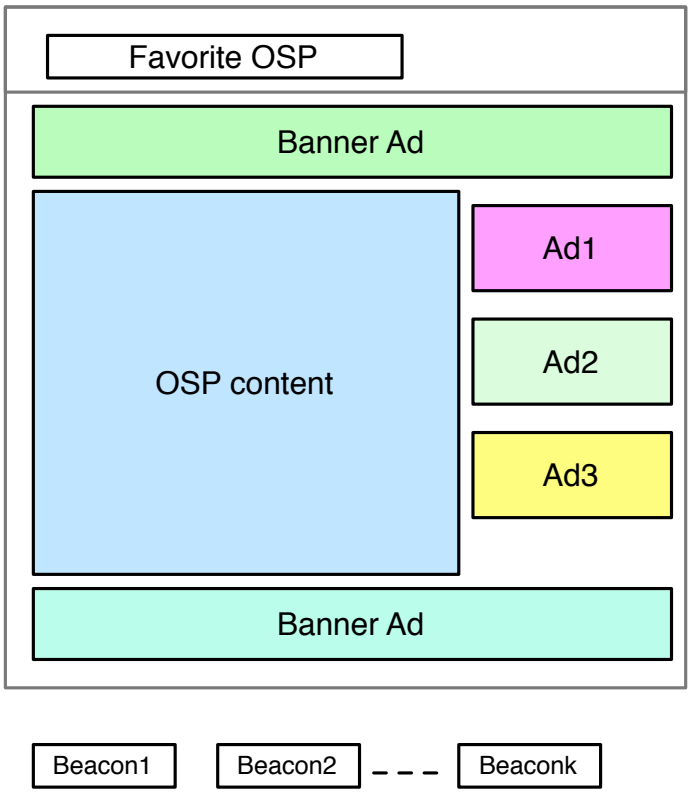
Tractability of Mixed Context

- Architectural dynamics defies establishing a trust relationship
  - Context different on each visit
  - Different actors “at the table”
- Lack of policy transitivity
  - OSP policy rooted in limiting liability
  - Contractual info absent



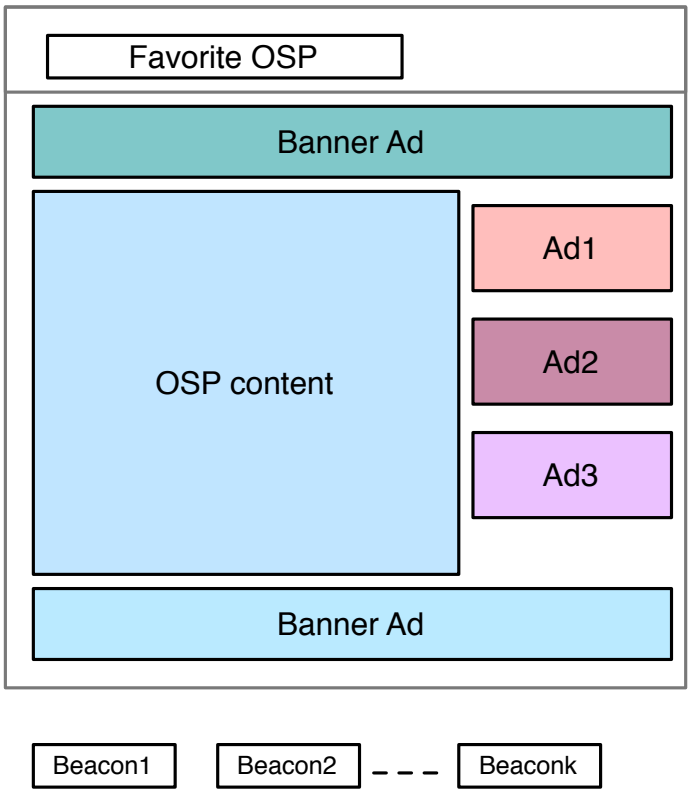
Tractability of Mixed Context

- Architectural dynamics defies establishing a trust relationship
  - Context different on each visit
  - Different actors “at the table”
- Lack of policy transitivity
  - OSP policy rooted in limiting liability
  - Contractual info absent



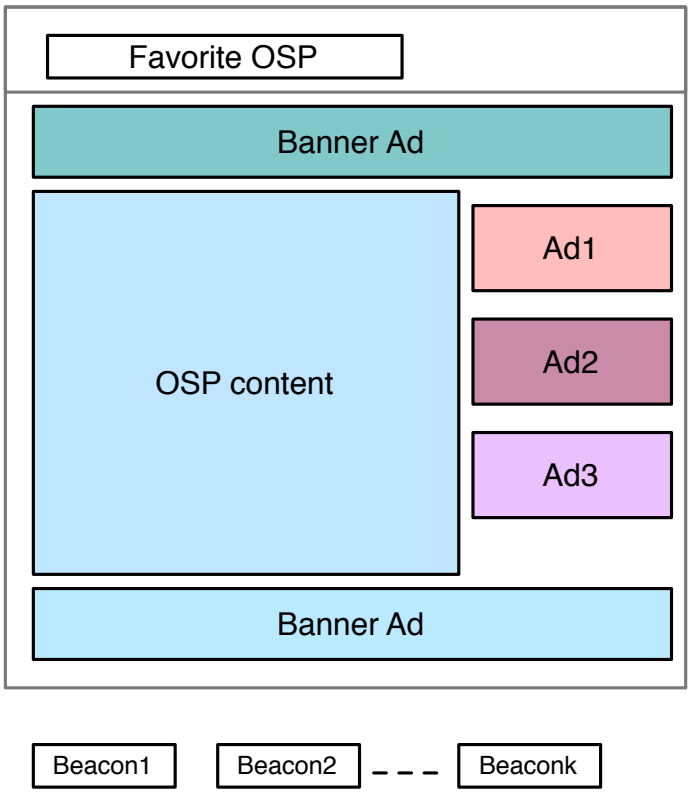
Tractability of Mixed Context

- Architectural dynamics defies establishing a trust relationship
  - Context different on each visit
  - Different actors “at the table”
- Lack of policy transitivity
  - OSP policy rooted in limiting liability
  - Contractual info absent



Tractability of Mixed Context

- Architectural dynamics defies establishing a trust relationship
  - Context different on each visit
  - Different actors “at the table”
- Lack of policy transitivity
  - OSP policy rooted in limiting liability
  - Contractual info absent



Context and Trust Revisited

Tractability issues ultimately undermine the ability to develop a genuine trust relationship with an OSP

Mixing Segments

- Segments considered non-PII

Mixing Segments

- Segments considered non-PII
  - age range, interest in wine, region, etc.

Mixing Segments

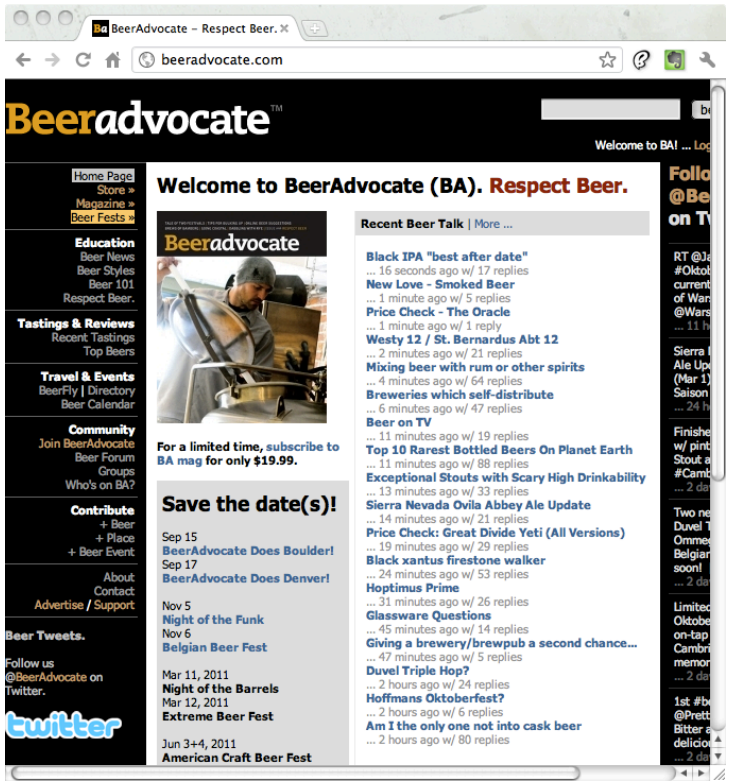
- Segments considered non-PII
  - age range, interest in wine, region, etc.
- Individually “innocuous”
- Together $\rightarrow$ aggregate image

Mixing Segments

- Segments considered non-PII
  - age range, interest in wine, region, etc.
- Individually “innocuous”
- Together $\rightarrow$ aggregate image
  - {age range, coarse locale, gender }

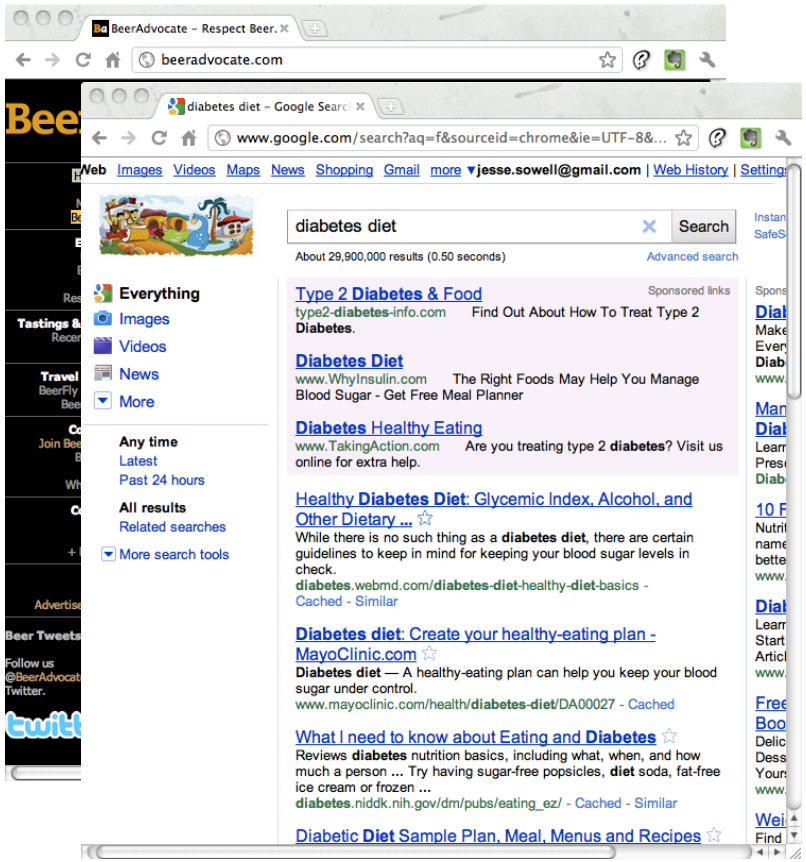
Mixing Segments

- Segments considered non-PII
  - age range, interest in wine, region, etc.
- Individually “innocuous”
- Together → aggregate image
  - {age range, coarse locale, gender brewing }



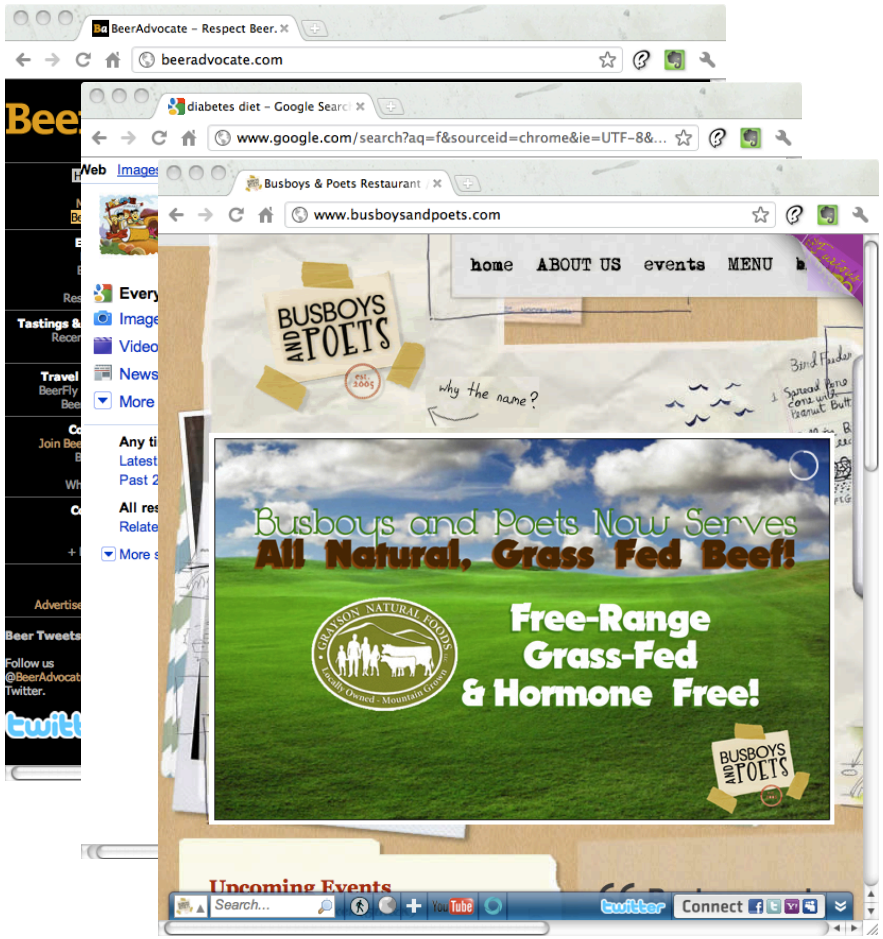
Mixing Segments

- Segments considered non-PII
  - age range, interest in wine, region, etc.
- Individually “innocuous”
- Together → aggregate image
  - {age range, coarse locale, gender brewing , diabetes, health }



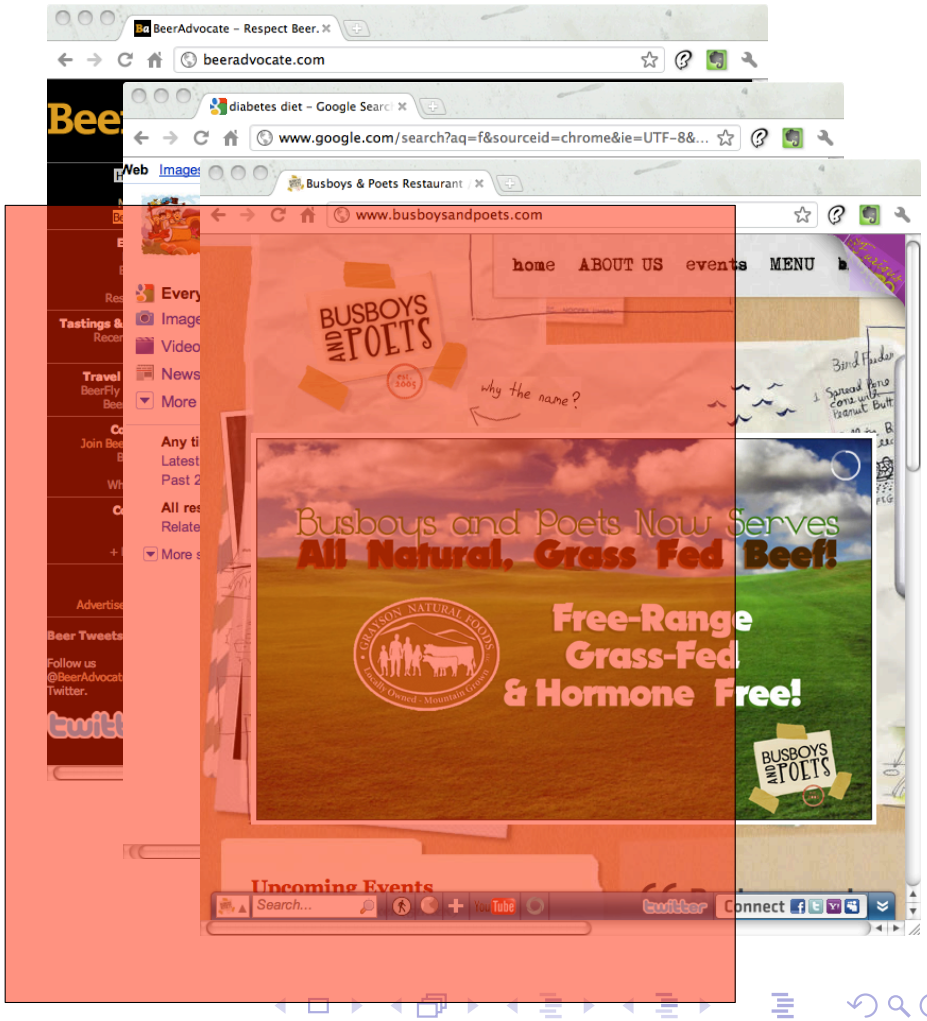
Mixing Segments

- Segments considered non-PII
  - age range, interest in wine, region, etc.
- Individually “innocuous”
- Together → aggregate image
  - {age range, coarse locale, gender brewing , diabetes, health , southern food, fried food }



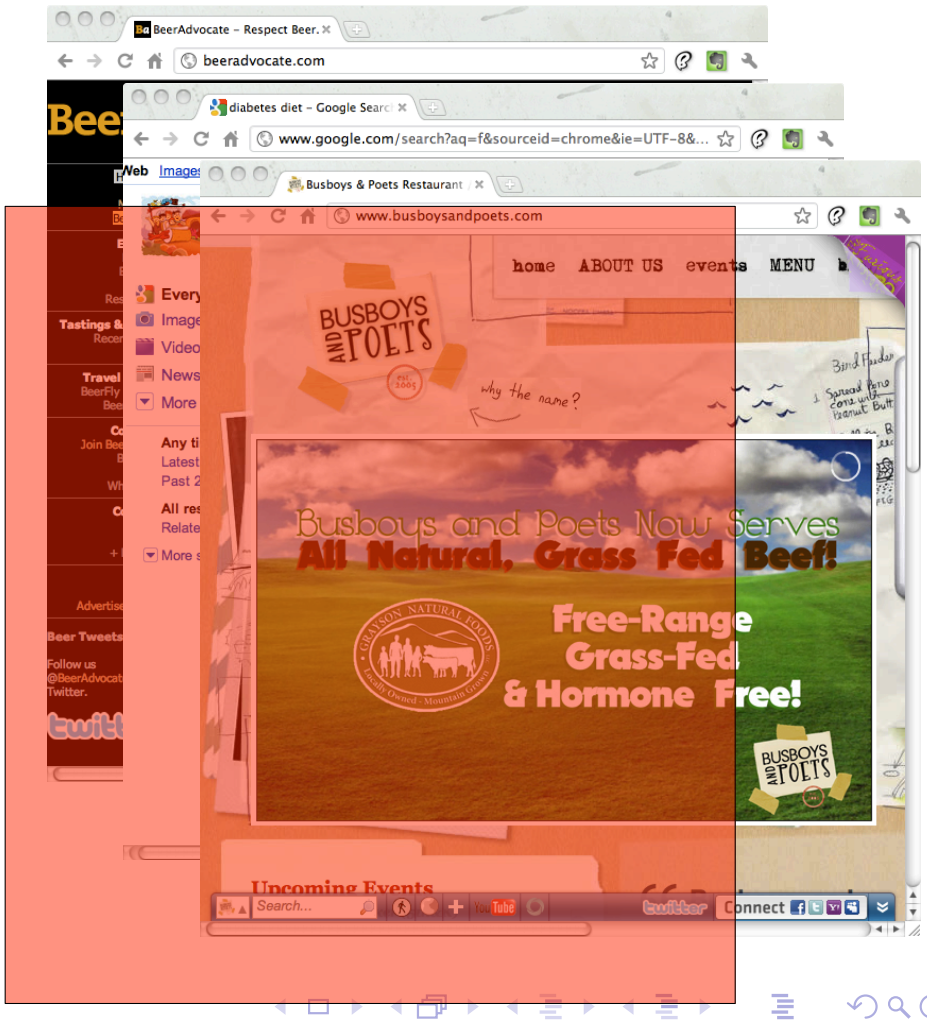
Mixing Segments

- Segments considered non-PII
  - age range, interest in wine, region, etc.
- Individually “innocuous”
- Together → aggregate image
  - {age range, coarse locale, gender brewing , diabetes, health , **diabetes supplies** , southern food, fried food }
- Next search for food may include diabetes supplies ad

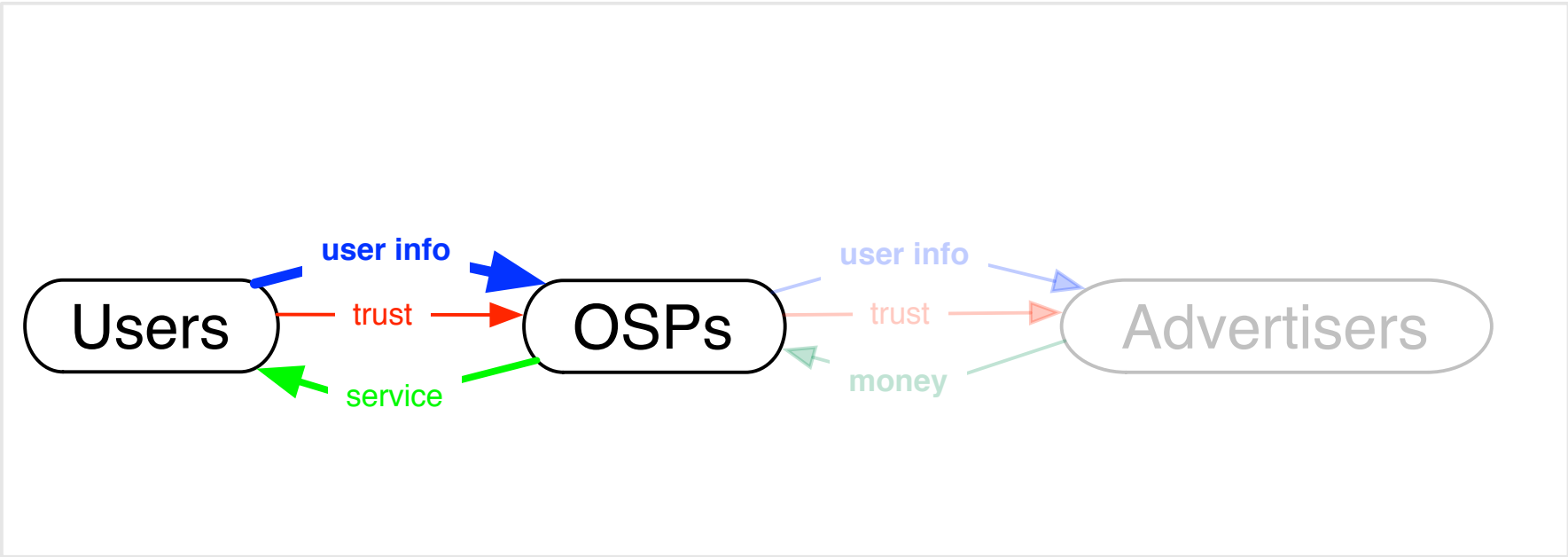


Mixing Segments

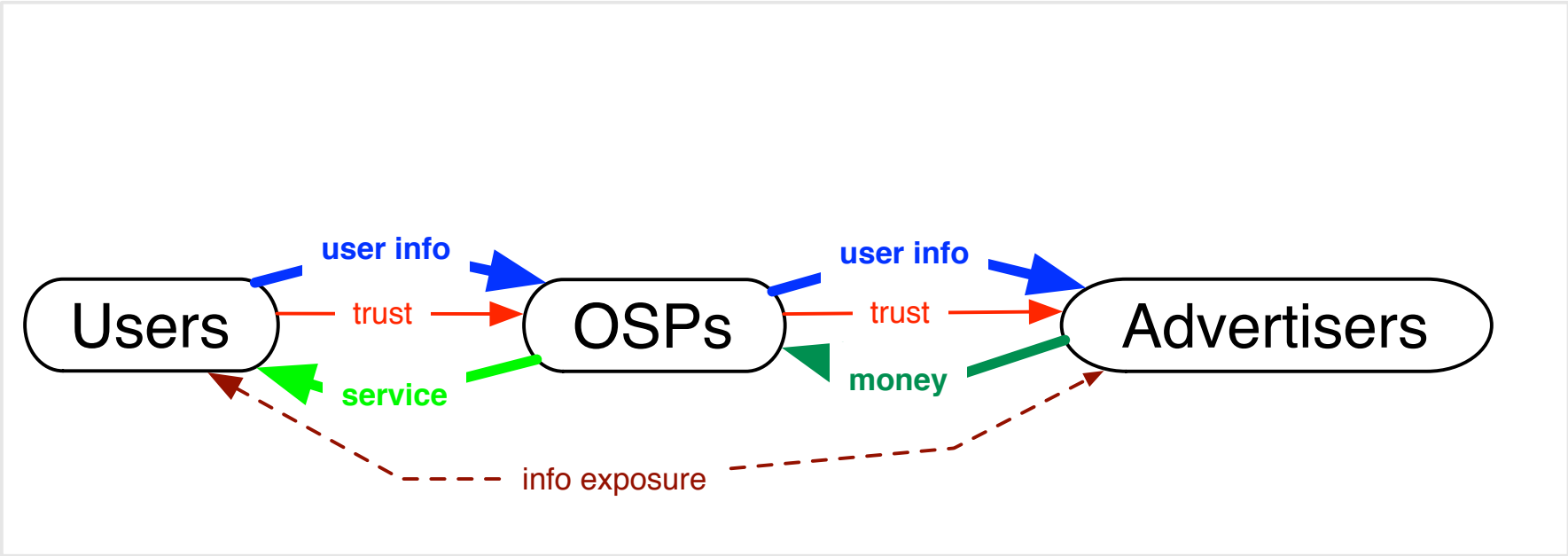
- Segments considered non-PII
  - age range, interest in wine, region, etc.
- Individually “innocuous”
- Together → aggregate image
  - {age range, coarse locale, gender brewing , diabetes, health , **diabetes supplies** , southern food, fried food }
- Next search for food may include diabetes supplies ad
- Privacy violation or appropriate mixing?
  - Depends on privacy preferences



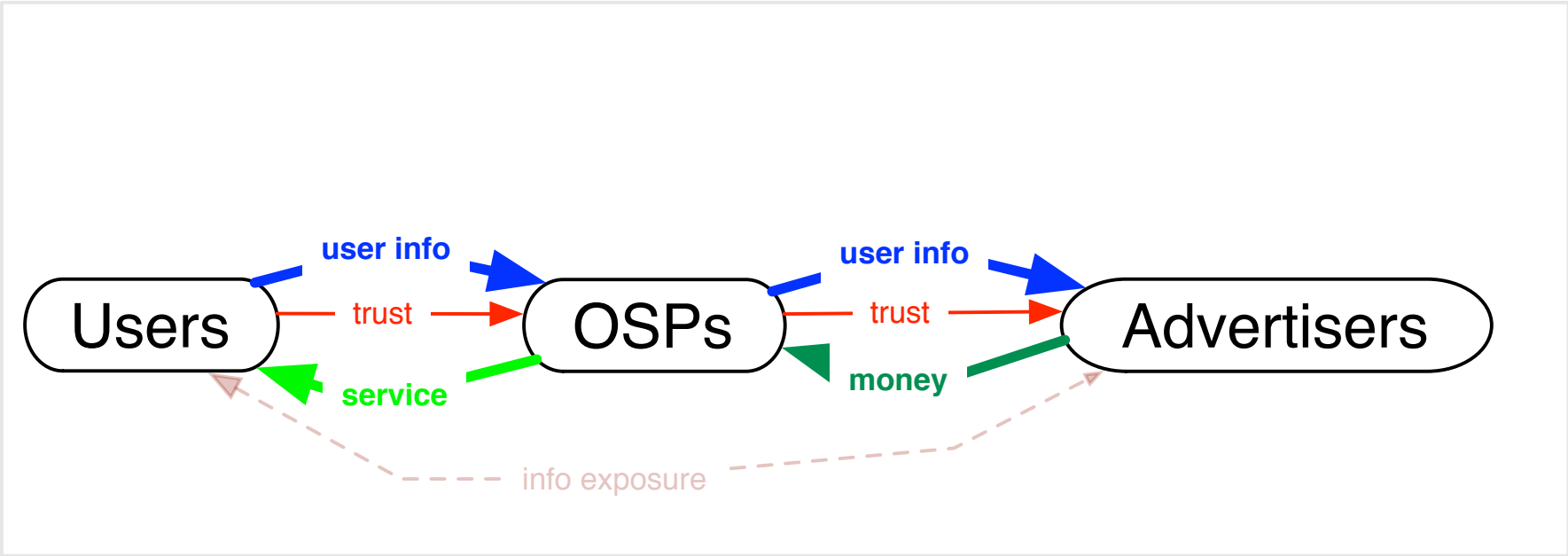
Who is at the Table?



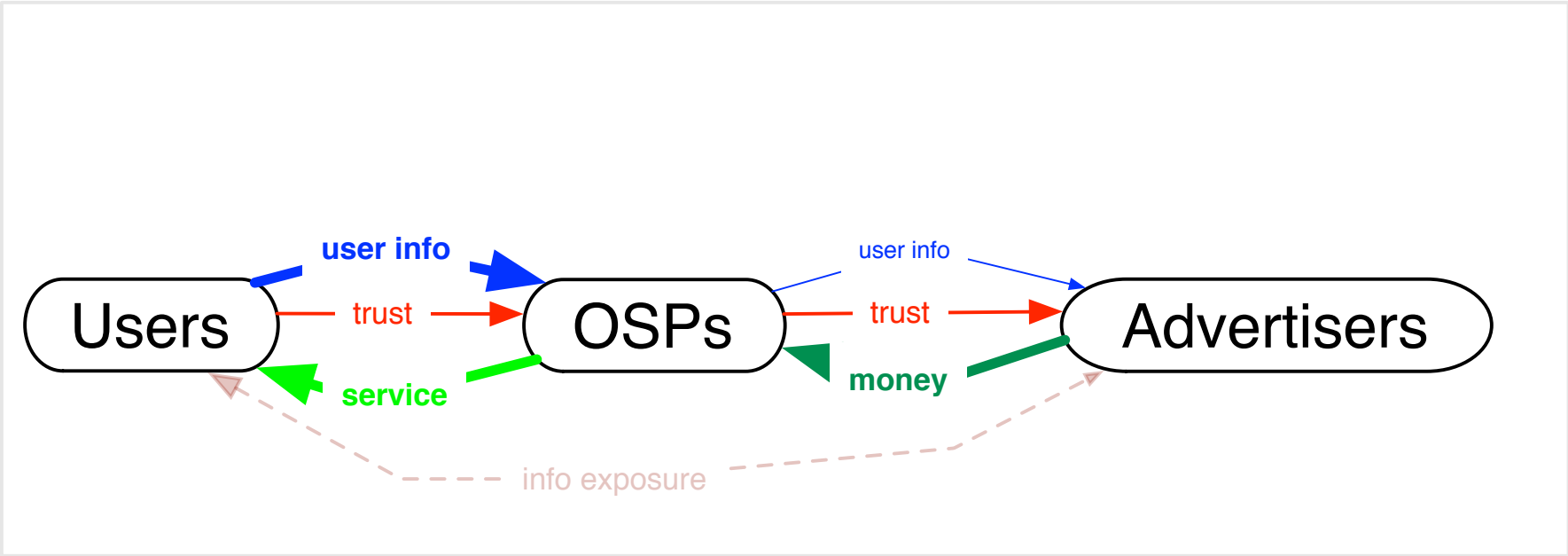
Who is at the Table?



Who is at the Table?



Who is at the Table?

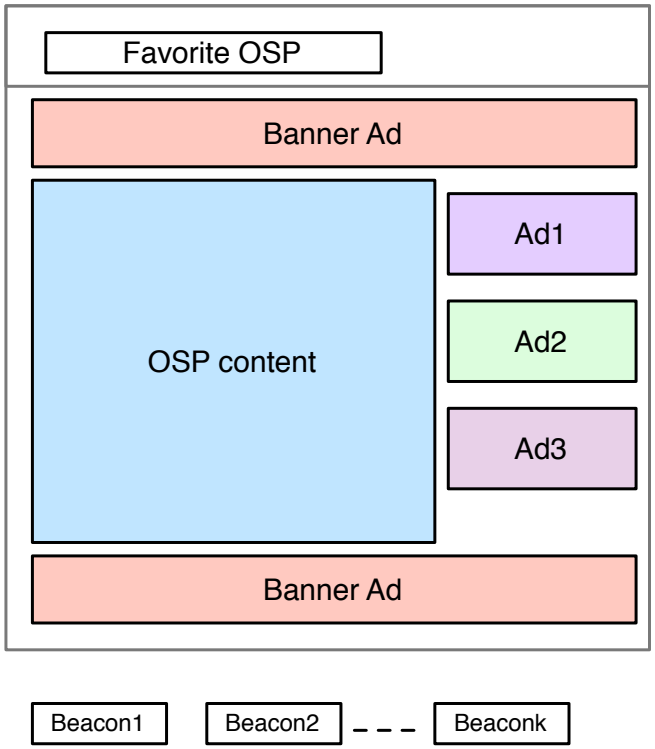


(Ideal) Recommendation?

Highlight Mixed Context

Augment architecture to make environment highlight context

- Ad networks' blue "i" a start
- Rating mechanism for ads
  - Data sharing amongst relevant actors
  - Natural experiments to collect actual preferences
- Advertiser reputation market
  - OSP rating transitivity
  - OSP-advertiser relationship

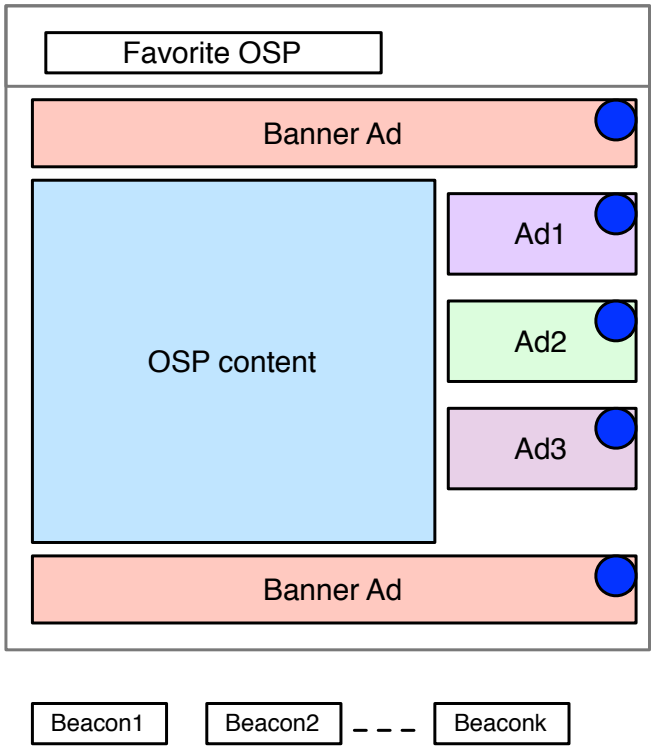


(Ideal) Recommendation?

Highlight Mixed Context

Augment architecture to make environment highlight context

- Ad networks' blue "i" a start
- Rating mechanism for ads
  - Data sharing amongst relevant actors
  - Natural experiments to collect actual preferences
- Advertiser reputation market
  - OSP rating transitivity
  - OSP-advertiser relationship

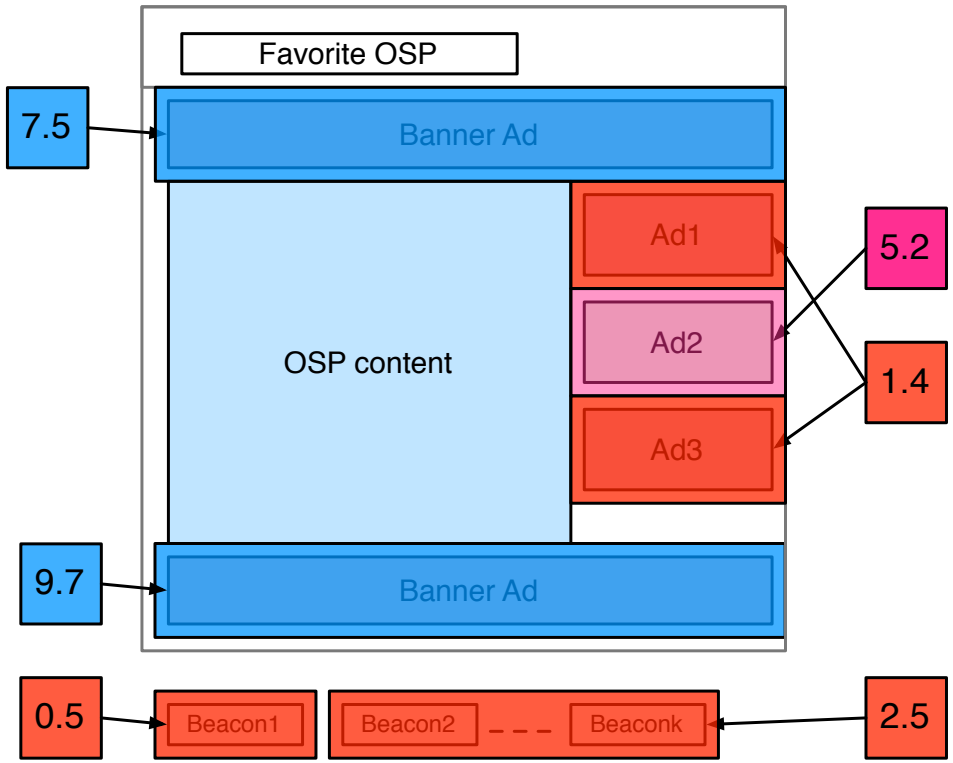


(Ideal) Recommendation?

Highlight Mixed Context

Augment architecture to make environment highlight context

- Ad networks' blue "i" a start
- Rating mechanism for ads
  - Data sharing amongst relevant actors
  - Natural experiments to collect actual preferences
- Advertiser reputation market
  - OSP rating transitivity
  - OSP-advertiser relationship

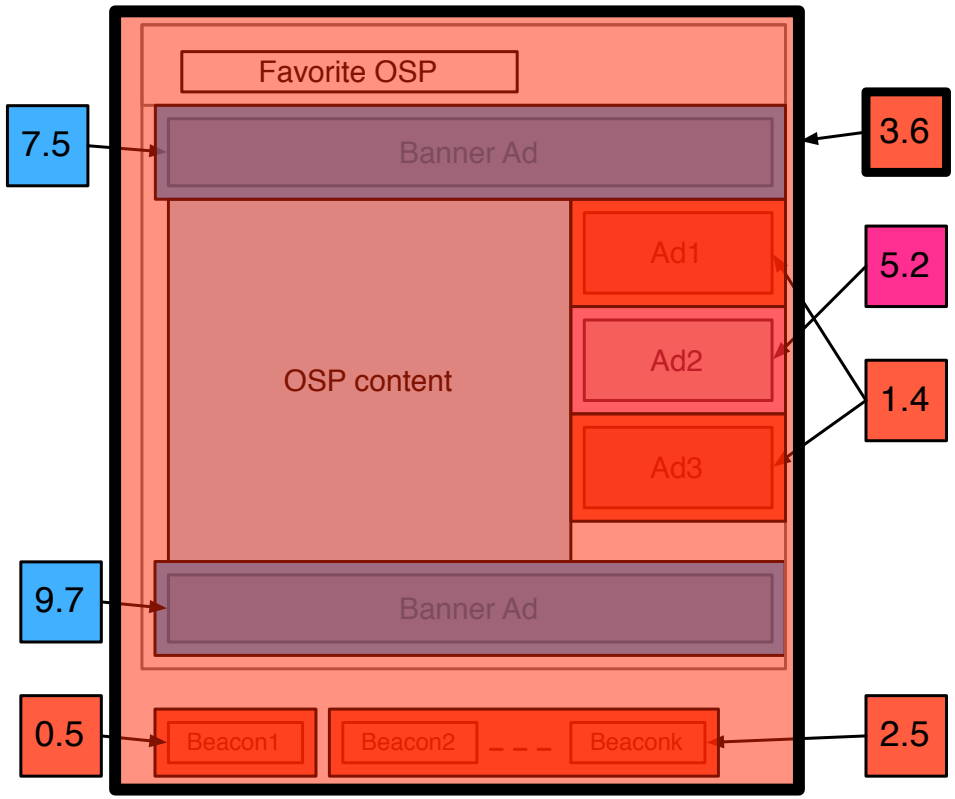


(Ideal) Recommendation?

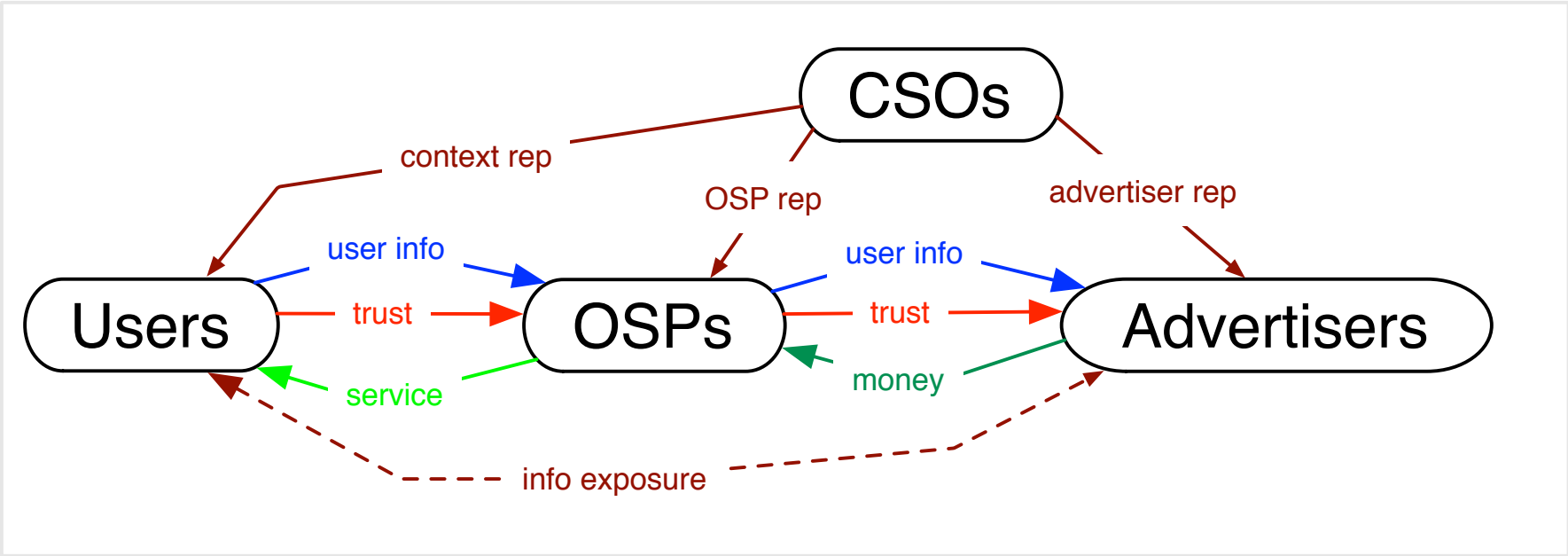
Highlight Mixed Context

Augment architecture to make environment highlight context

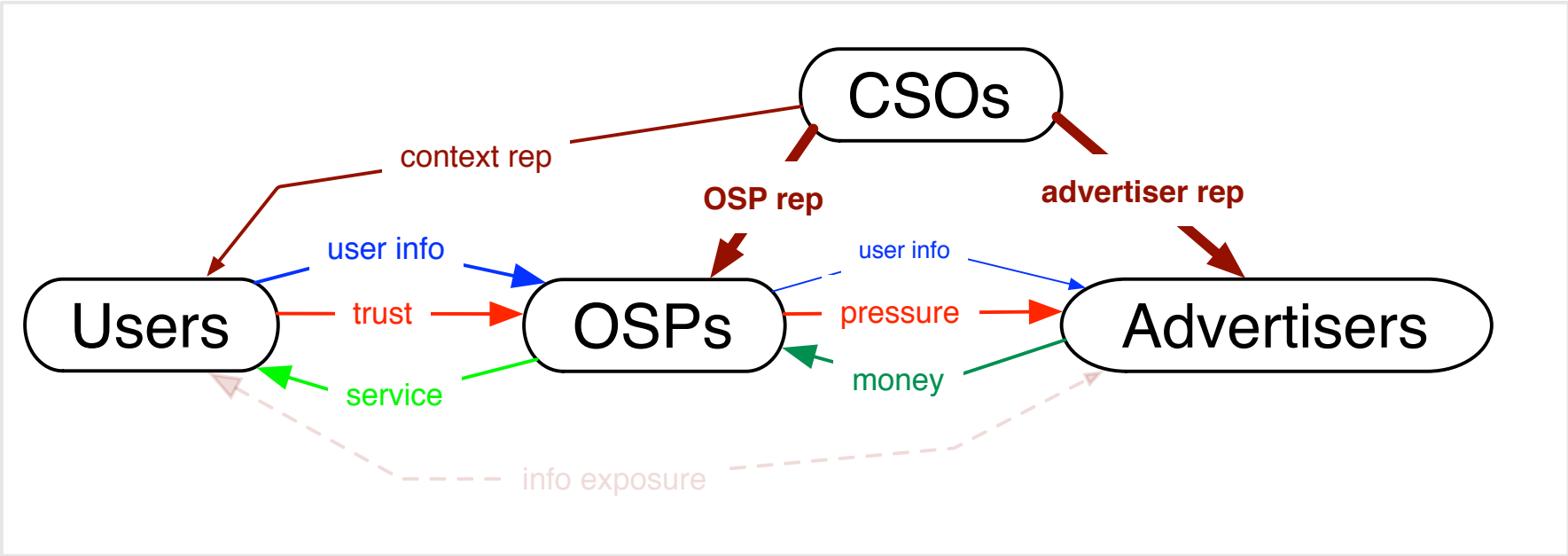
- Ad networks' blue "i" a start
- Rating mechanism for ads
  - Data sharing amongst relevant actors
  - Natural experiments to collect actual preferences
- Advertiser reputation market
  - OSP rating transitivity
  - OSP-advertiser relationship



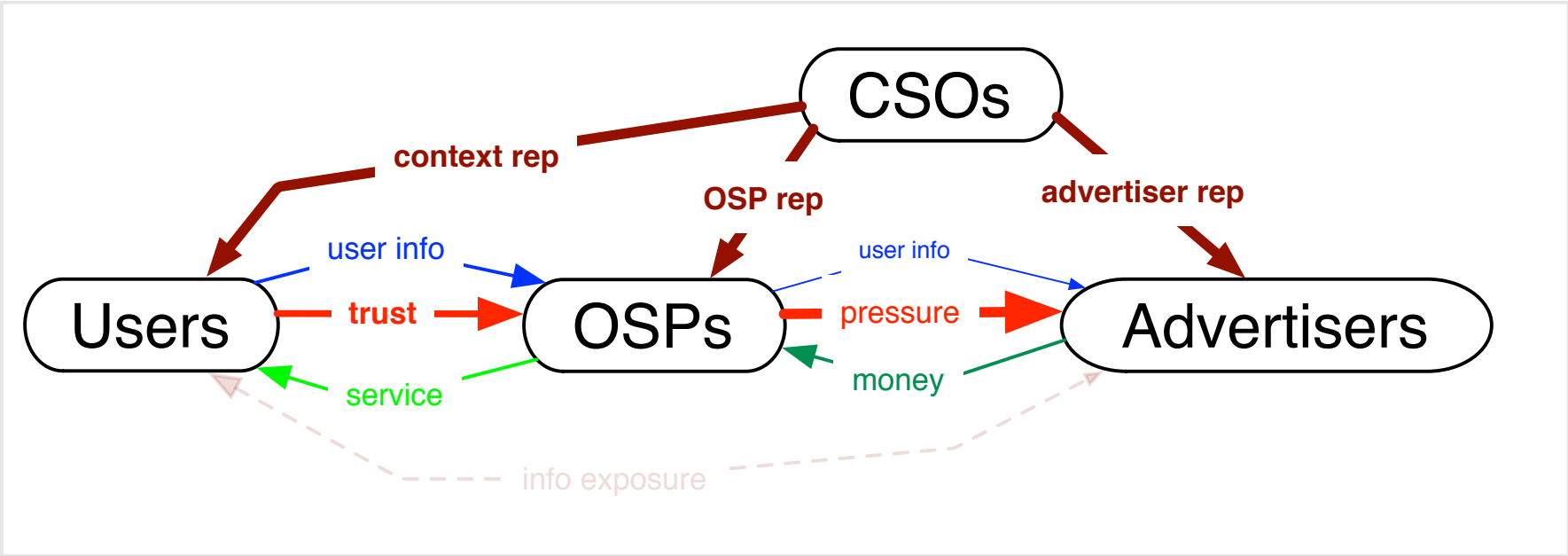
The CSO Option



The CSO Option



The CSO Option



How Idealistic?

- Back to initial questions . . .
  - What is the role of regulatory bodies?
  - What is missing from this hybrid regime?
    - Self-reinforcing mechanisms . . .
  - What are the politically and strategically feasible incentive structures for developing supporting metrics?
- A few more . . .
  - "Ideal" CSO solution is one particular end point
  - *Are there* there politically and strategically feasible options? How can we tell?
  - What characterizes the collection of entry points to a critical path to this type of collaborative solution?
  - How can we use this to compare options?