What is validity?

- **Coherence theory** – a knowledge claim is true, if it belongs to a coherent set of claims; e.g., smoking marijuana causes cancer
- **Correspondence theory** – a knowledge claim is true, if it corresponds to the world; e.g., it’s sunny outside

Coherence by example

Barth et al.’s 2006 formalization of contextual integrity…

- Begins with a philosophical abstraction, hypothesis or stated assumption, i.e., Contextual Integrity defined by Nissenbaum
- Establishes a coherent working example: Alice and Bob exchanging information about Charlie
- Establishes central concepts and rules of inference in Temporal Logic
- Claims fit prevailing assumptions about the world:
  “These norms are interpreted in a model of communicating agents who ‘respect’ the norms if the trace history of their communication satisfies a temporal formula constructed from the norms by taking the disjunction over positive norms and the conjunction over negative norms.”


Correspondence by example

May et al.’s 2006 formalization of regulatory privacy rules…

- Begins with a research claim… that HIPAA consent rules can be expressed using access control matrix operations
- Establishes method with heuristics to translate English legal text into rules expressed in Promela
  - **Heuristic #1**: bi-directional tracing of legal cross-references to logic
  - **Heuristic #2**: distinguish system state and environmental state; latter is only known to human operators (e.g., testimonials)
- Results include select boundary cases and method limitations

Correspondence by example

Breaux et al.’s 2006 formalization of HIPAA...

- Begins with open coding frame to identify rules and constraints, multiple analysts compared coding result
- Establishes method with heuristics to translate English legal text into rules expressed in first order logic
  - Heuristic #1: definitions express transitive hierarchy of concepts
  - Heuristic #2: reconciling and prioritizing legal exceptions
  - Heuristic #3: conflicts due to rule subsumption
  - Heuristic #4: explicate implied rights from stated obligations
- Results include specific technical challenges to formalization


Threats to validity

Construct Validity: does the formal semantics accurately reflect the problem semantics?

External Validity: to what extent is the data representative of the problem at large?

Internal Validity: are the inferences drawn from the dataset consistent and complete?

Reliability: can multiple people apply the method to yield the same results?

(1) \([O_1]\) The covered entity \([C_1]\) who has a direct treatment relationship with the individual must...
   (A) Provide notice \([C_2]\) no later than the first service delivery;

(2) For the purposes of paragraph (1), \([O_2]\) a covered entity \([C_3]\) who delivers services electronically must provide electronic notice unless... \([C_4]\)

- From paragraph (1) we extracted \(O_1: [C_1 \land C_2]\)
- Now we carry down \(C_1, C_2, C_3\) from paragraph (1) to yield \(O_2: [C_1 \land C_2 \land C_3 \land \neg C_4]\)
The diagram illustrates the Requirements Exception Hierarchy as per IEEE TSE ‘08. It shows how data storage devices and facsimiles are categorized under different requirements and exemptions. The language employs distributed controls to shape conditionality. Definitions and exemptions shape who, when, and how requirements are applied in practice. The Nevada Chapter 603a, Security of Personal Information, provides the context for these requirements. The diagram is a visual representation of the complex regulations and exceptions that govern personal information security.
### Conclusions

- Coherence alone cannot guarantee privacy; conformance is burdensome, but critical
- Claims of “compliance” with policy are human interpretations of complex situations
- Decision makers (human interpreters) are needed to resolve policy conflicts