Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

An Ontological Analysis of Privacy Threat Impact

Habtamu Abie, PhD
Senior Researcher – DART
Norwegian Computing Center

PETweb Workshop
Oslo December 11, 2007

Outline

- What is the problem area of interest?
- How can we increase awareness and understanding of privacy?
- Why an ontological privacy threat impact analysis?
- Privacy impact analysis prototype

The problem area of interest

- The web makes it easy to access data and easy to aggregate and correlate data from numerous different sources
- The advent of more complex services that involve multiple service providers (SPs) exacerbates the privacy concerns
- As it raises the potential of personal information being shared across these providers in ways that weren't intended by the owner of the information

The problem area of interest…

- Primarily interested in privacy preservation in the context of such complex services that involve multiple SPs
  - envision that such services are realized by composing component services, each of which may be provided by a different provider

- Does privacy mean so many different things to so many different people?
  - “How can privacy be addressed in a manner that is non-reductive and contextual,
  - yet simultaneously useful in deciding cases and making sense of the multitude of privacy problems we face?”

Understanding privacy

- A structure that may be helpful in an overall understanding of privacy is thus sorely needed
  - Taxonomy and Ontology are two of such structure
- Taxonomy is the practice and science of classification
  - helps to give a more structured view of the topic at hand
- Taxonomy of privacy
  - characterization of the various notions of privacy
  - identify and understand the different kinds of socially recognized privacy violations
  - focus more specifically on the different kinds of activities that impinge upon privacy
  - aid in the development of the law that addresses privacy (purpose)
  - be helpful in an overall understanding of privacy to support implementation issues in next generation privacy aware information systems

Understanding privacy: taxonomy

- The goal is to define more precisely
  - what the problem is in each context
  - how it is unique
  - how it differs from other problems
  - how it is related to other types of privacy problems

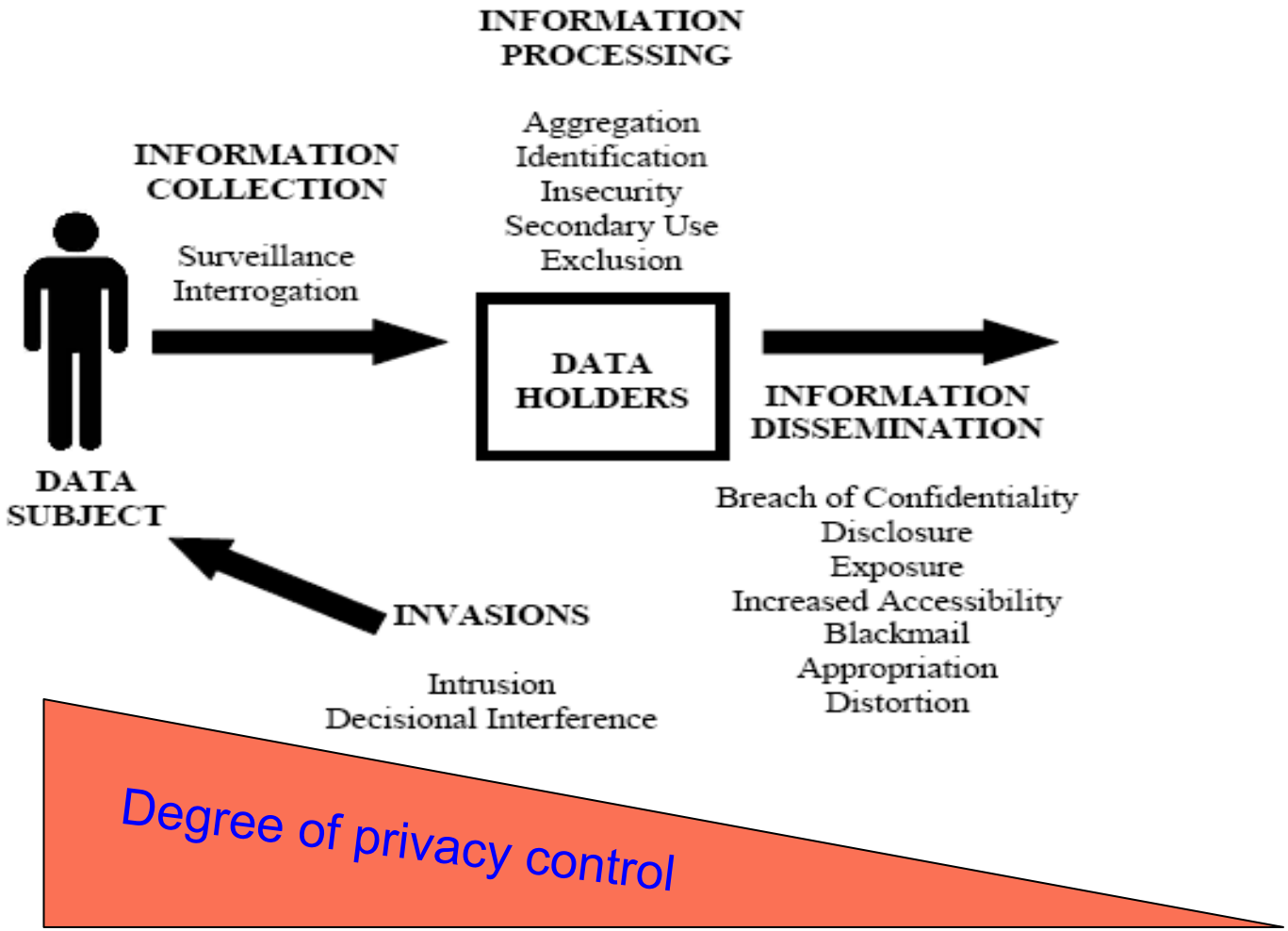
- There are four basic groups of harmful activities
  - (1) information collection
  - (2) information processing
  - (3) information dissemination
  - (4) invasion - involves impingement directly on the individual

  - Each of these groups consists of different related subgroups of harmful activities

Source: Daniel J. Solove, A Taxonomy of Privacy

A taxonomy of privacy model

- The progression from information collection to processing to dissemination is the data moving further away from the control of the data subject
- In principle an individual has some control about what is collected
- **less** about how it is processed
- **very little** as it becomes more widely disseminated



Why an ontological privacy threat impact analysis?

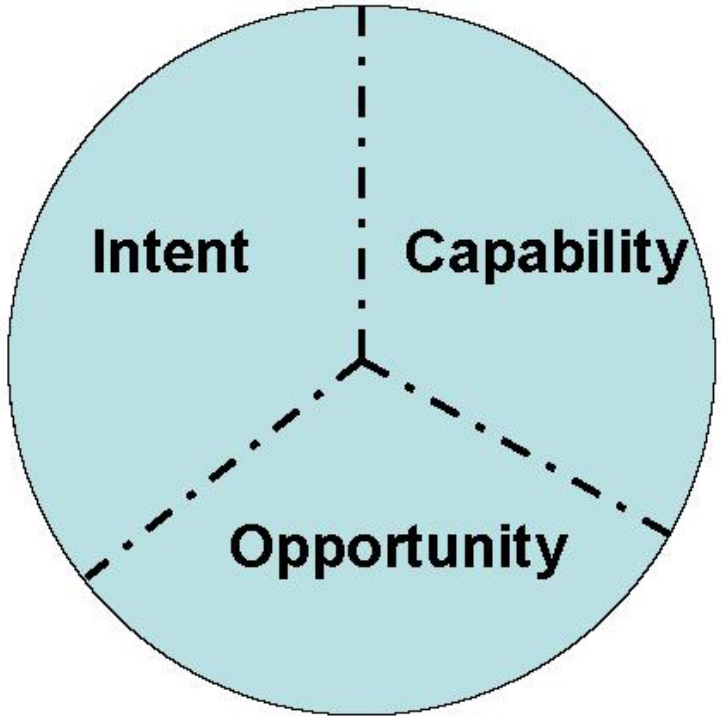
- Risk analysis is one of the techniques used to measure the strength of the protection mechanisms
  - an estimation of the probability of specific threats, vulnerabilities and their consequences and costs
- Threat analysis is the first step in risk analysis
  - for the identification of sources and types of threats and their likelihood
- Ed Felten's wise advice on the importance of threat analysis
  - *"The first rule of security analysis is this: understand your threat model. Experience teaches that if you don't have a clear threat model - a clear idea of what you are trying to prevent and what technical capabilities your adversaries have - then you won't be able to think analytically about how to proceed. The threat model is the starting point of any security analysis."*

Privacy threat ontology

- An ontology is an explicit specification of a conceptualization
  - A conceptualization is an abstract, simplified view of the world that we wish to represent for some purpose
  - A study of conceptions of reality and the nature of being
  - Formally, an ontology is the statement of a logical theory
  - In computer science and information science, an ontology is a data model that represents a set of concepts within a domain and the relationships between those concepts
- An ontology of privacy threats, then, is
  - an explicit specification of a conceptualization of privacy threats,
  - including the threat actors, actions, and threat target objects that establish the relationships of their production, use, and destruction

Threat elements as Tripartite integrated whole

- **Ontological structure of threats as integrated wholes possessing three inter-related parts**
  - **Intentional**
  - **Capabilities**
  - **Opportunities**
- **Shows how these elements stand to**
  - **one another**
  - **conditions of vulnerabilities**



Metaphysical relations such as foundational dependence

Source:

- E. G. Little and G. L. Rogova, An ontological analysis of threat and vulnerability

- S. Vidalis and A. Jones, Analyzing threat agents & their attributes

Threat agent attributes

- **Intentional - the degree to which an agent is prepared to implement a threat**
  - Intentions are plans or goals to be accomplished.
  - They represent the psychological component of threats
  - Can be deeply influenced by one's capabilities and opportunities (e.g., determining soft vs. hard targets)

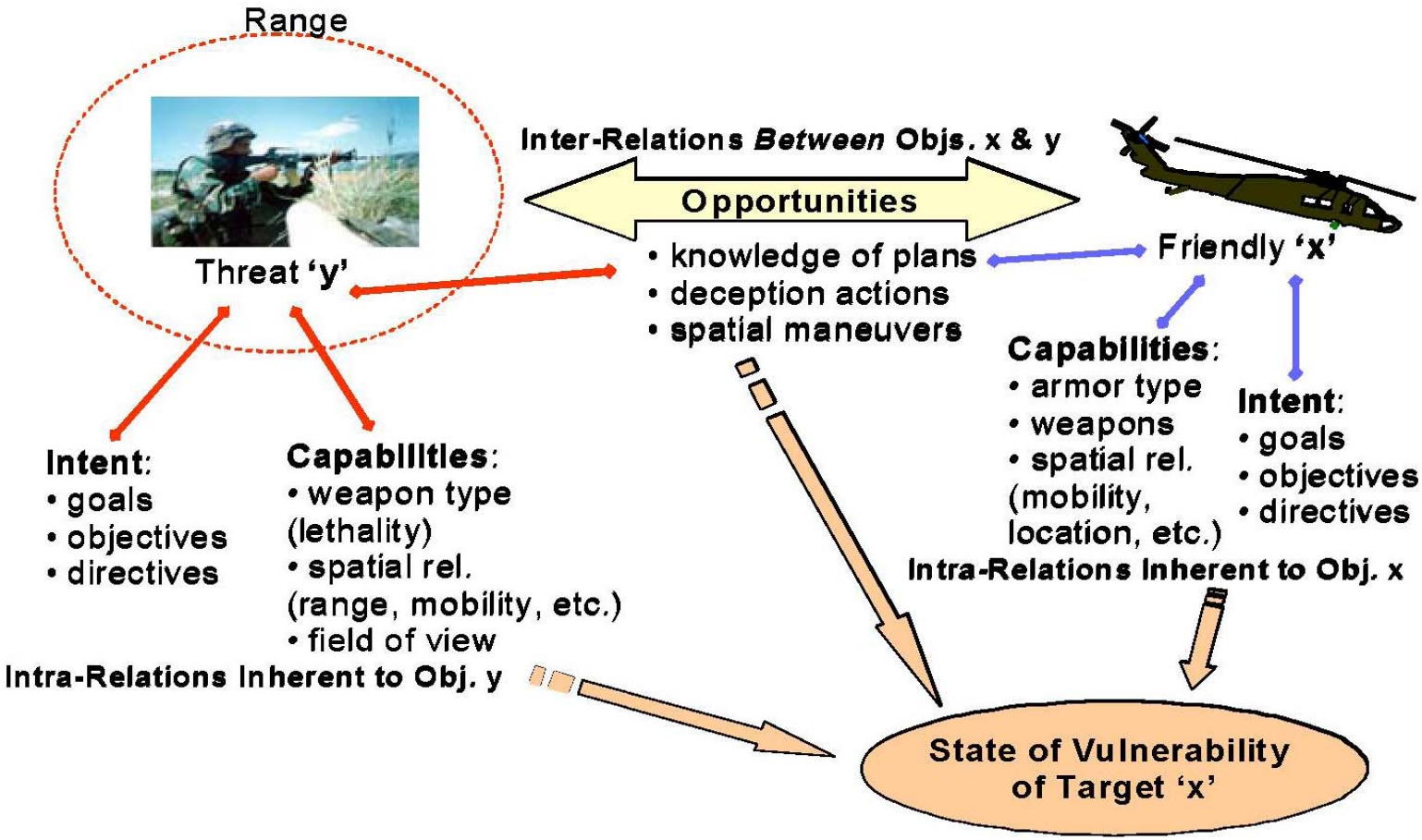
- **Capabilities (i.e., capacities) - the degree to which a threat agent is able to implement a threat**
  - the kinds of objects (e.g., weapons),
  - object attributes (e.g., projectile or explosive abilities) or
  - behaviors (e.g., movements, perceptual abilities)
  - can inflict a certain level of harm, disruption or lethality on some target (as identified by one's intentions and made available by opportunities)

Threat agent attributes…

- **Opportunities - a favorable occasion for action**
  - the spatio-temporal states of affairs like a line of sight to the target, access to a person or facility, abilities to know the adversary's plans (intentions).

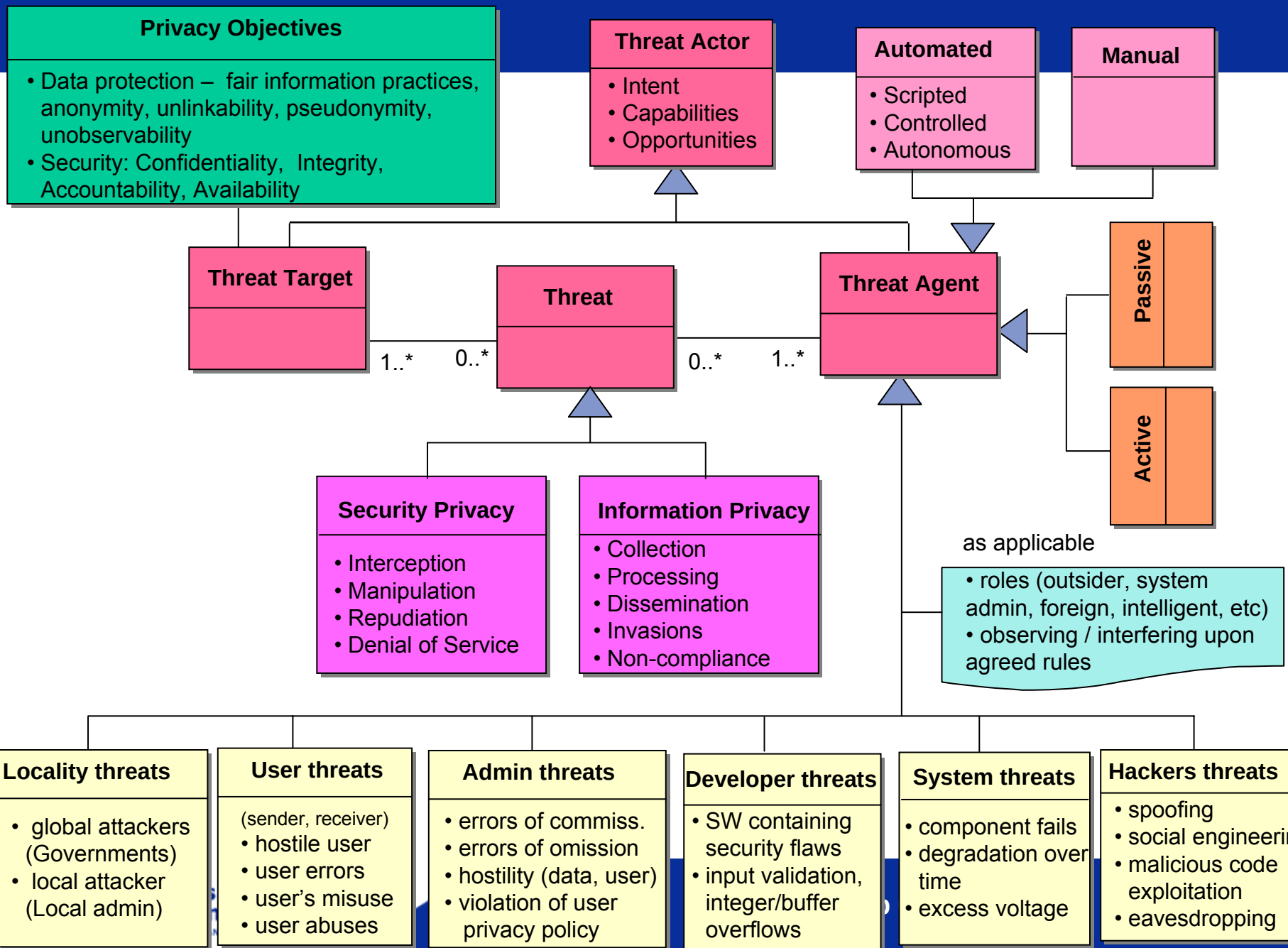
- **Opportunities** make it possible to actualize (i.e., carry out) one's intent given sufficient capabilities.

Inter- and intra-relational structures of vulnerabilities

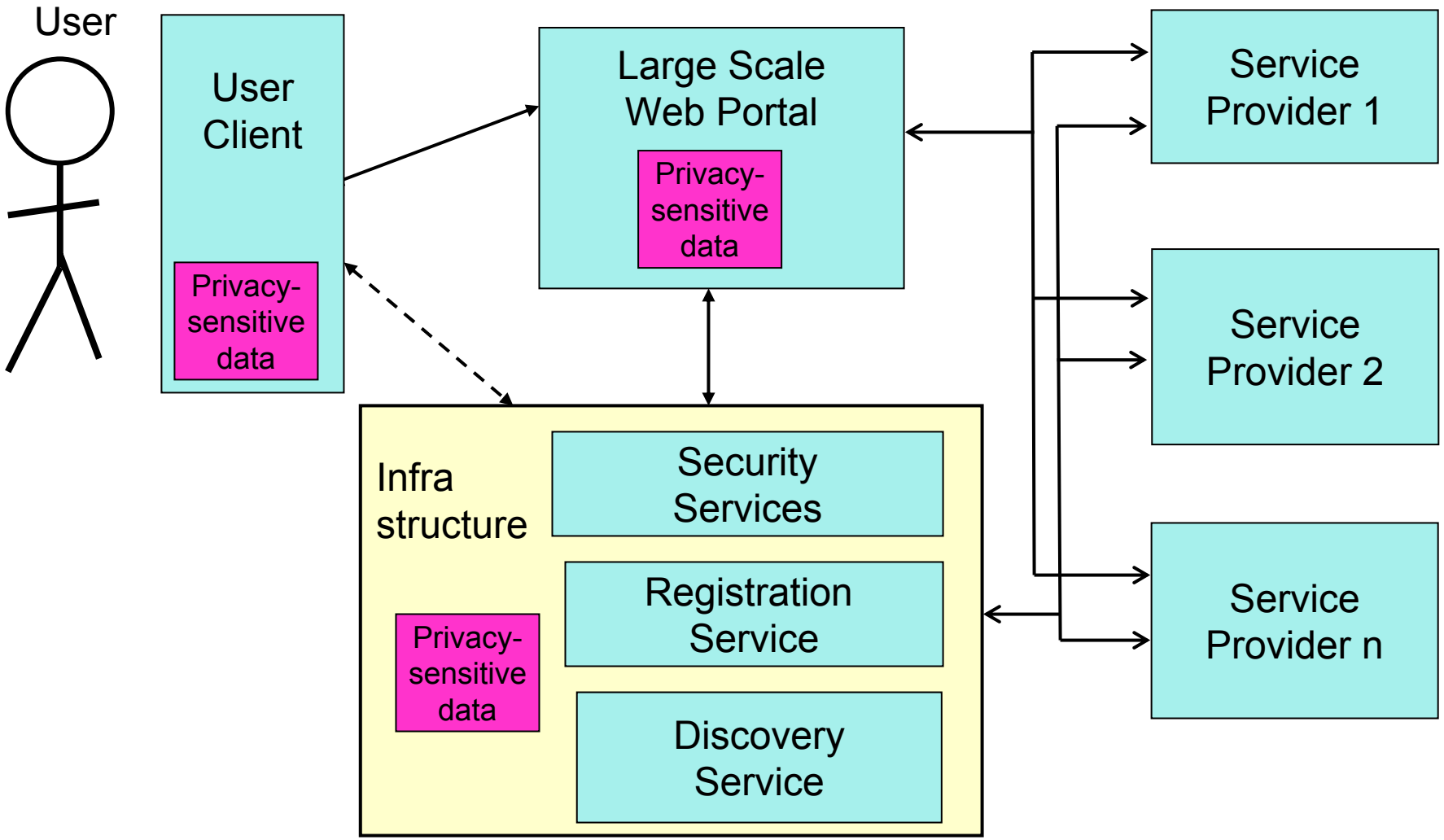


Source: E. G. Little and G. L. Rogova, An Ontological analysis of Threat and Vulnerability

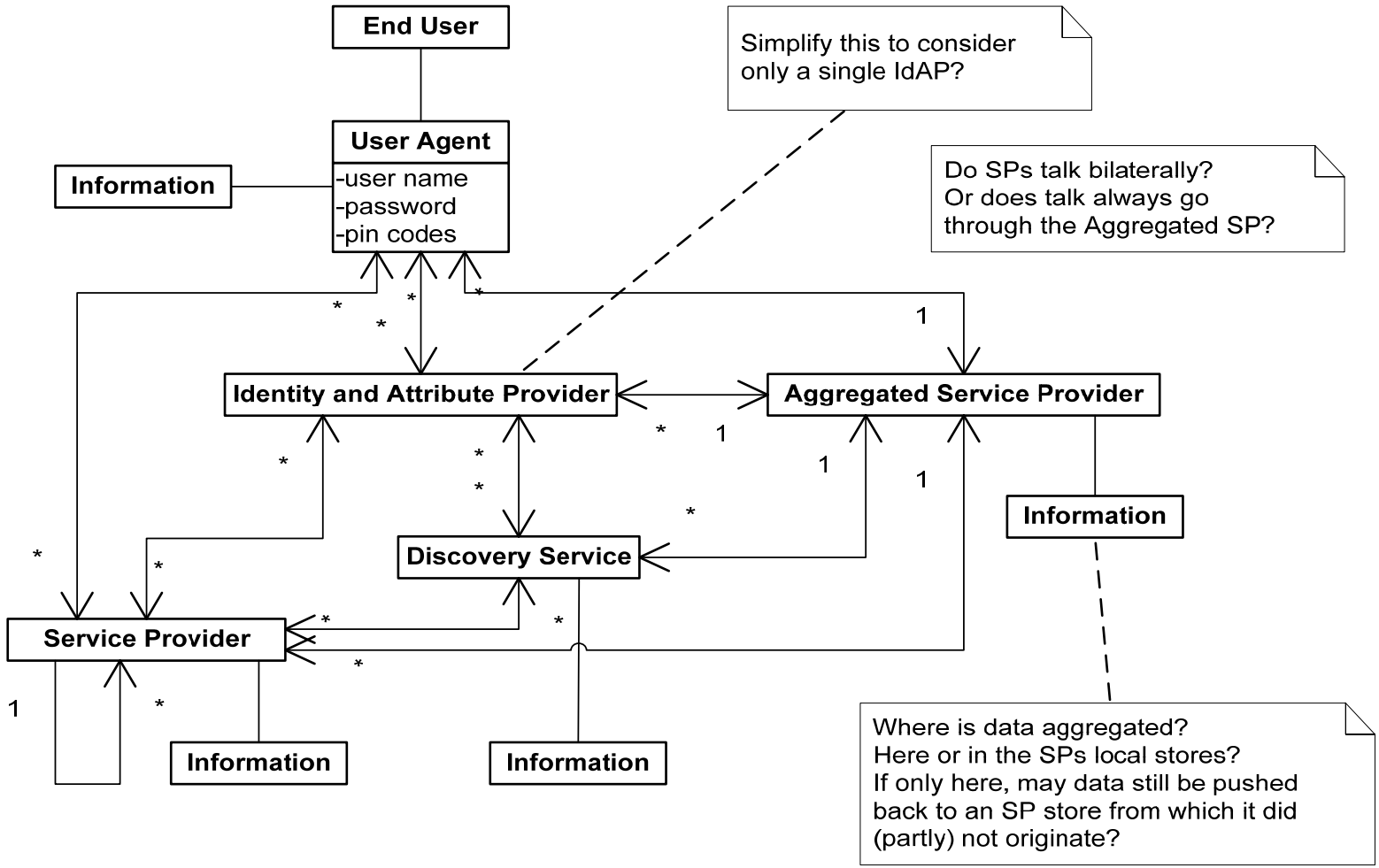
Privacy threats ontology



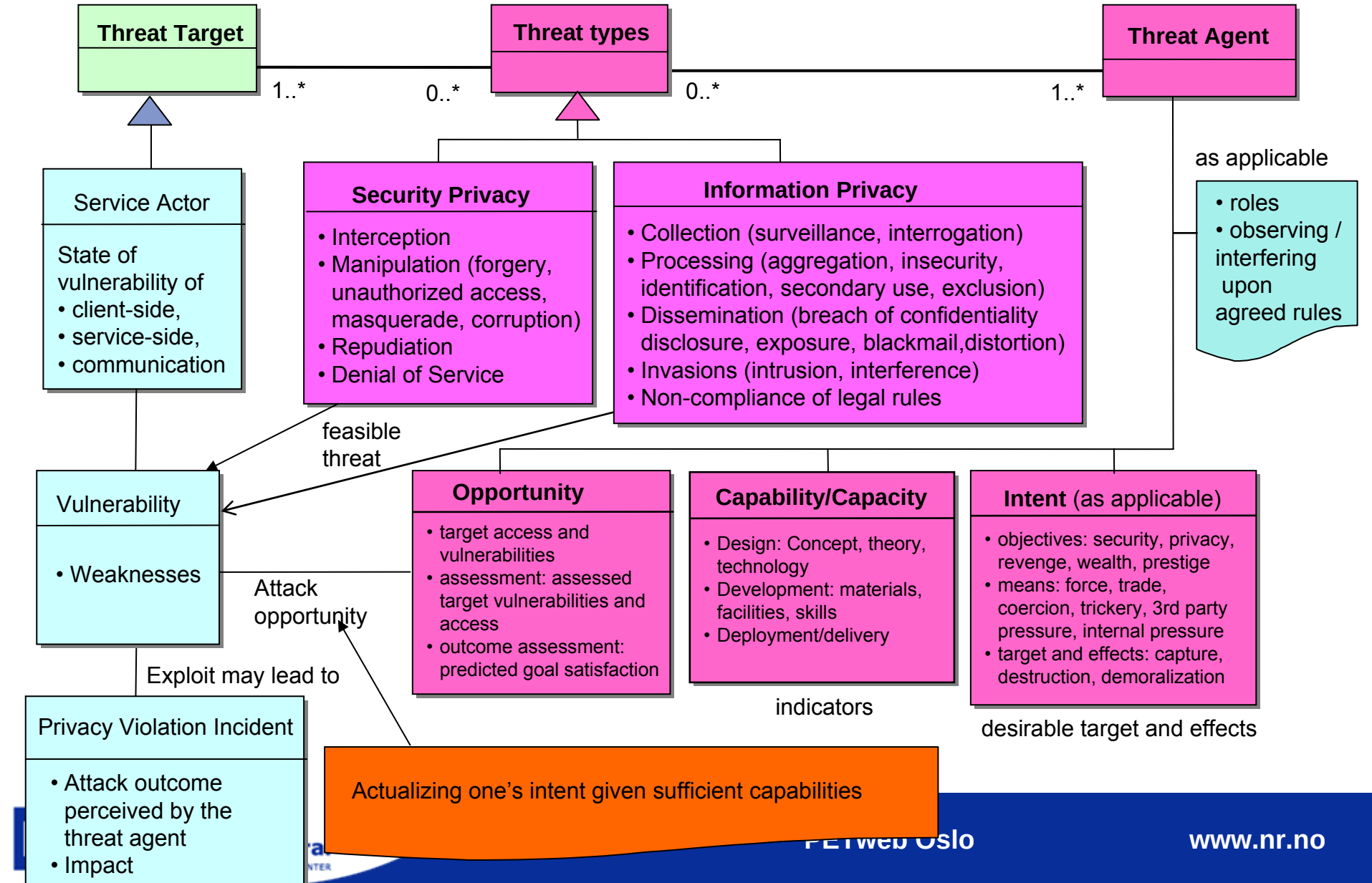
Architecture for PETweb w/SSO



System architecture for aggregated services



Ontological analysis of privacy threat impact



Privacy threat impact calculation

- Asset - threat target
  - End user, user agent, Id provider, SP, ASP, DiscServ
- Locality Access
  - Local, global, physical, logical
- Threat agents
  - Locality (global/local), user, admin, developers, system, hackers
- Motives
  - Intent, capability, opportunity
- Threats
  - security/data protection

Privacy threat impact calculation…

- **Outcome**
  - disclosure, modification

- **Ranking the impact** of the threat being realized

  0 = Not applicable to privacy

  1 = Insignificant – Negligible impact on privacy

  2 = Minor – Minor impact on privacy

  3 = Moderate – Medium impact on privacy

  4 = Major – Major impact on privacy

  5 = Disastrous – Comprehensive impact on privacy

Privacy impact analysis prototype

	A	B	C	D	E	F
1	Number	Asset Name		Asset Individual Rating	Asset Weight	Contrib. to system Rating
2	1	End User (EU)		100	10,00 %	10
3						
4						
5		Threat Agent type		Impact Score	Threat Weight	Threat weighted Score
6		Hacker threats		5,00	20	100
7						
8		Threat Description				
9		This measures to what extent a Hacker is a threat to the User Agent and the information on it.				
10						
11			Attacks originating from a Hacker			
12			Social engineering			
13		Likelihood	0,00			
43						
44		Consequence/Outcome	5			
45						
46		- Security Privacy	5			
47		Interception	2			
48		Manipulation	5			
49		Denial of service	1			
50		Repudiation	2			
51						
52		- Information Privacy	3			
53		**Information collection**				
54		Surveillance	2			
55		Interrogation	1			
56		**Information processing**				
57		Aggregation	2			
58		Identification	1			
59		Insecurity	1			
60		Secondary use	1			
61		Exclusion	1			
62		**Infomation dissemination**				
63		Breach of confidentiality	2			
64		Disclosure	3			
65		Exposure	2			
66		Increased accessibility	2			
67		Blackmail	1			
68		Appropriation	2			

System Overview | Impact Score Overview | **Asset 1 EU** | Asset 2 UA | Asset 3 IAP | Asset 4 DS | Asset 5 ASP | Ass

The End

- **Thanks for your attention!**