A Graphic Expression for Privacy Claims

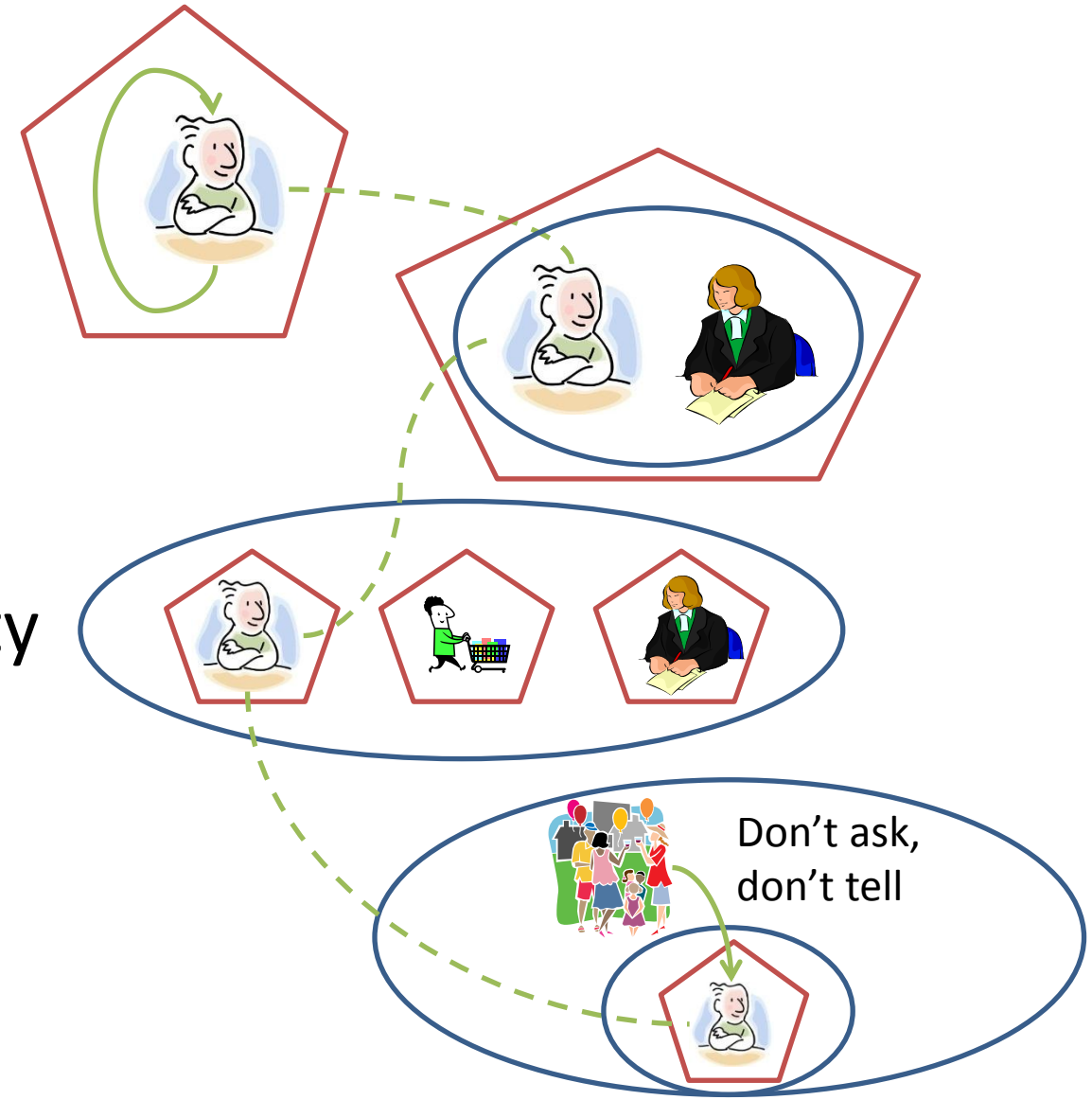
Clark Thomborson
The University of Auckland
20 June 2012

Designing for Privacy

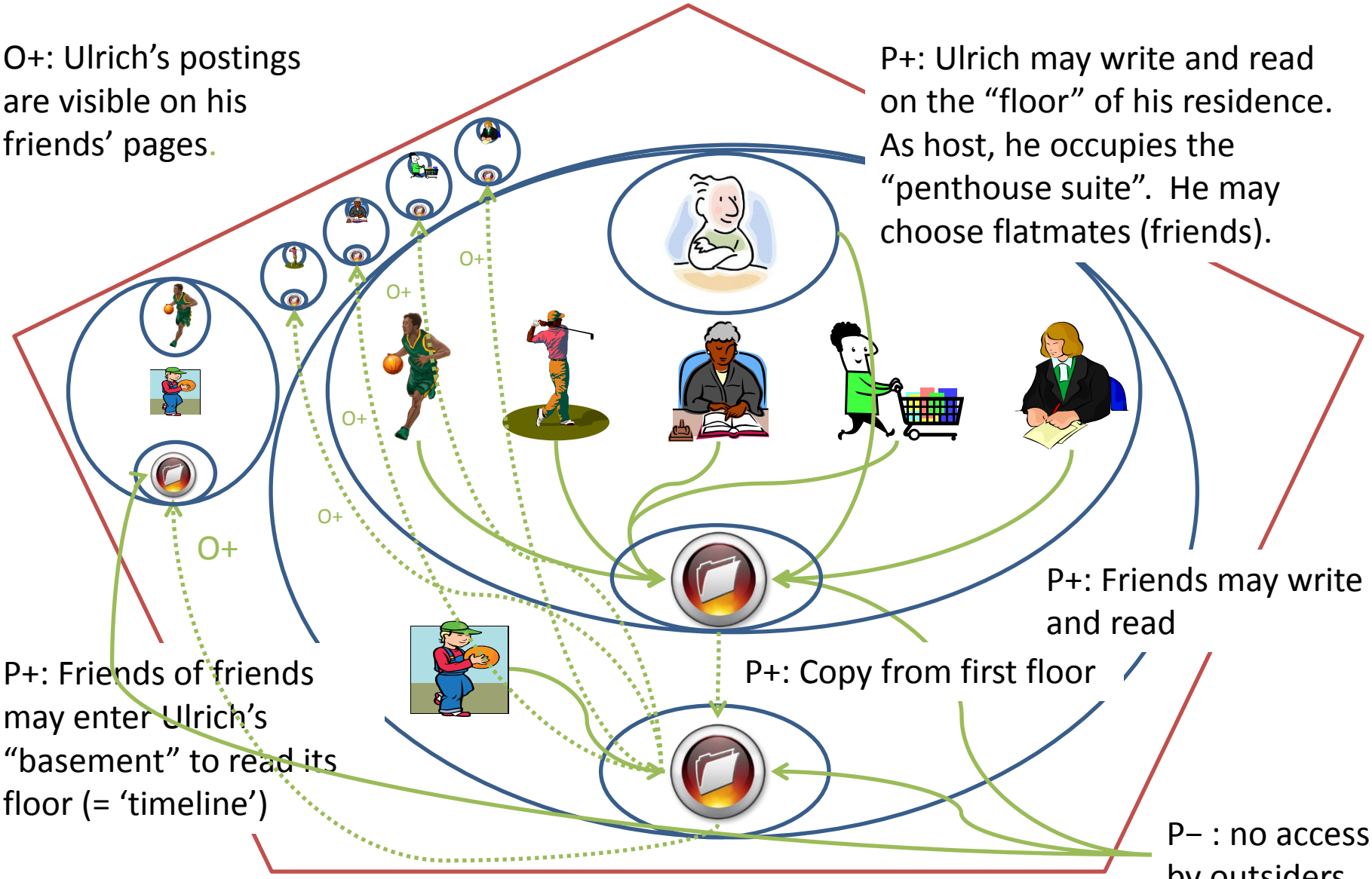
- If a computerised system supports privacy, what should it do? What shouldn't it do?
  - "Privacy" varies greatly, depending on the legal, cultural, individual, and organisational context.
- What are the design elements, and the design patterns, for a privacy-supportive system architecture?
  - Stakeholders define "what is required" (privacy laws, claims, preferences, …).
  - Architects know "what is possible".
- What is a good language for "architectural sketches"?
  - Sketches should depict legal, cultural, individual, and organisational requirements for a system, in its context.
  - Sketches should be evocative, not complicated.

Westin's "Four Basic States of Privacy"

1. Solitude
2. Intimacy
3. Anonymity
4. Reserve



Facebook

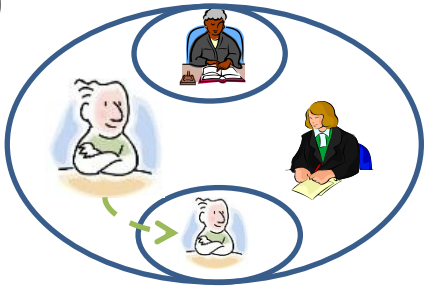

O+: Ulrich's postings are visible on his friends' pages.
P+: Ulrich may write and read on the "floor" of his residence. As host, he occupies the "penthouse suite". He may choose flatmates (friends).
O+
O+
O+
O+
O+
P+: Friends may write and read
P+: Copy from first floor
P+: Friends of friends may enter Ulrich's "basement" to read its floor (= 'timeline')
P– : no access by outsiders

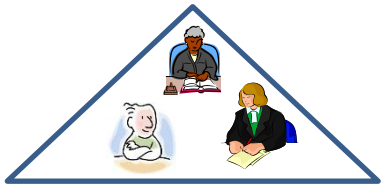
Model Elements

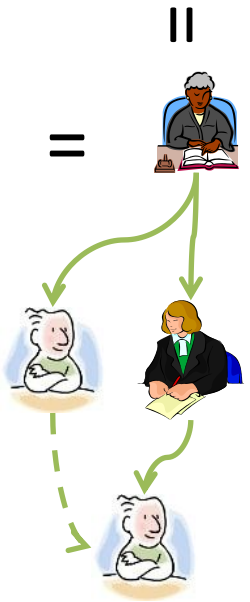
- Pentagon: a privacy claim (P- to outside access)
  - P+, P-: Permitted, prohibited actions
  - O+, O-: Obligated, exempted actions
  - R+, R-: Recommended, deprecated actions
- Solid arrow: “superior” to “inferior”
  - control (write), and observe (read)
- Dotted arrow: “master copy” to “partial copy”
  - Dotted line indicates equality
- Dashed line: “aliases”, “personae”, “aspects”
  - Equivalent to a solid line and a dotted line (bidirectional control + copy relations)

Model Elements (2)

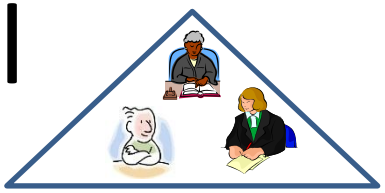
- Pentagon: a private area (P- to outside access)
  - Specific claims are shown by labels on arrows
- Ellipse: a communication area (a “peerage”)
  - Top: controller or “overlord”
  - Middle: “peers” (can read & write to bottom)
  - Bottom: “the commons” (a wiki for peers)
- Triangle: a “hierarchy”
  - Superior at top, inferiors below
- Icons: persons, data, automata
  - Dashed arrow: partial persona (a psuedonym)
- Models are a statement of fact or belief.
  - Different stakeholders have different models!





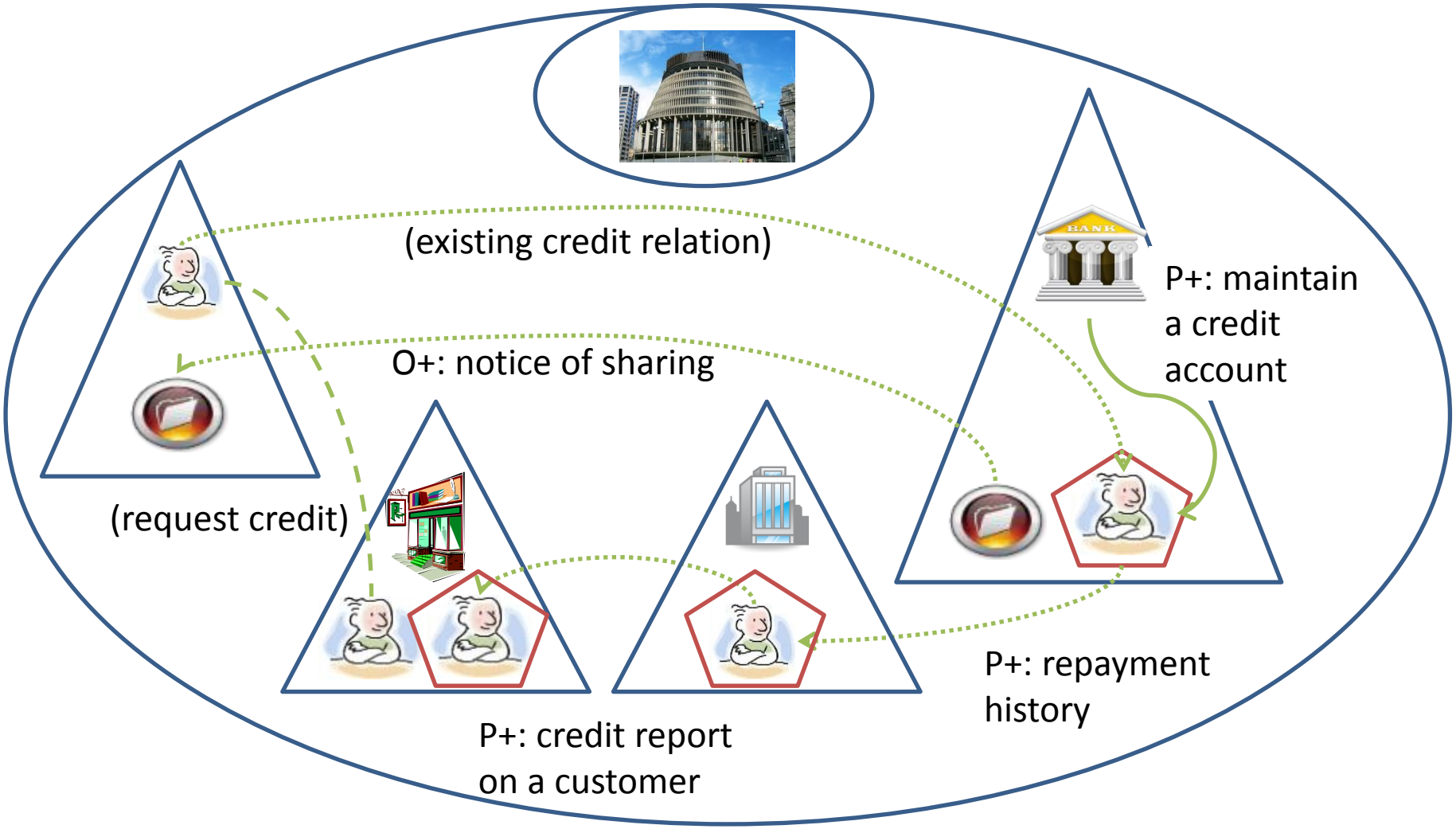


Semantics of Control



- Inferior actors may act against their superior's prospective controls (laws, orders, instructions, constraints).
- Inferiors are subject to observation and retrospective controls (punishments & rewards) by their superior.
- Rights may be granted to an inferior by a superior.

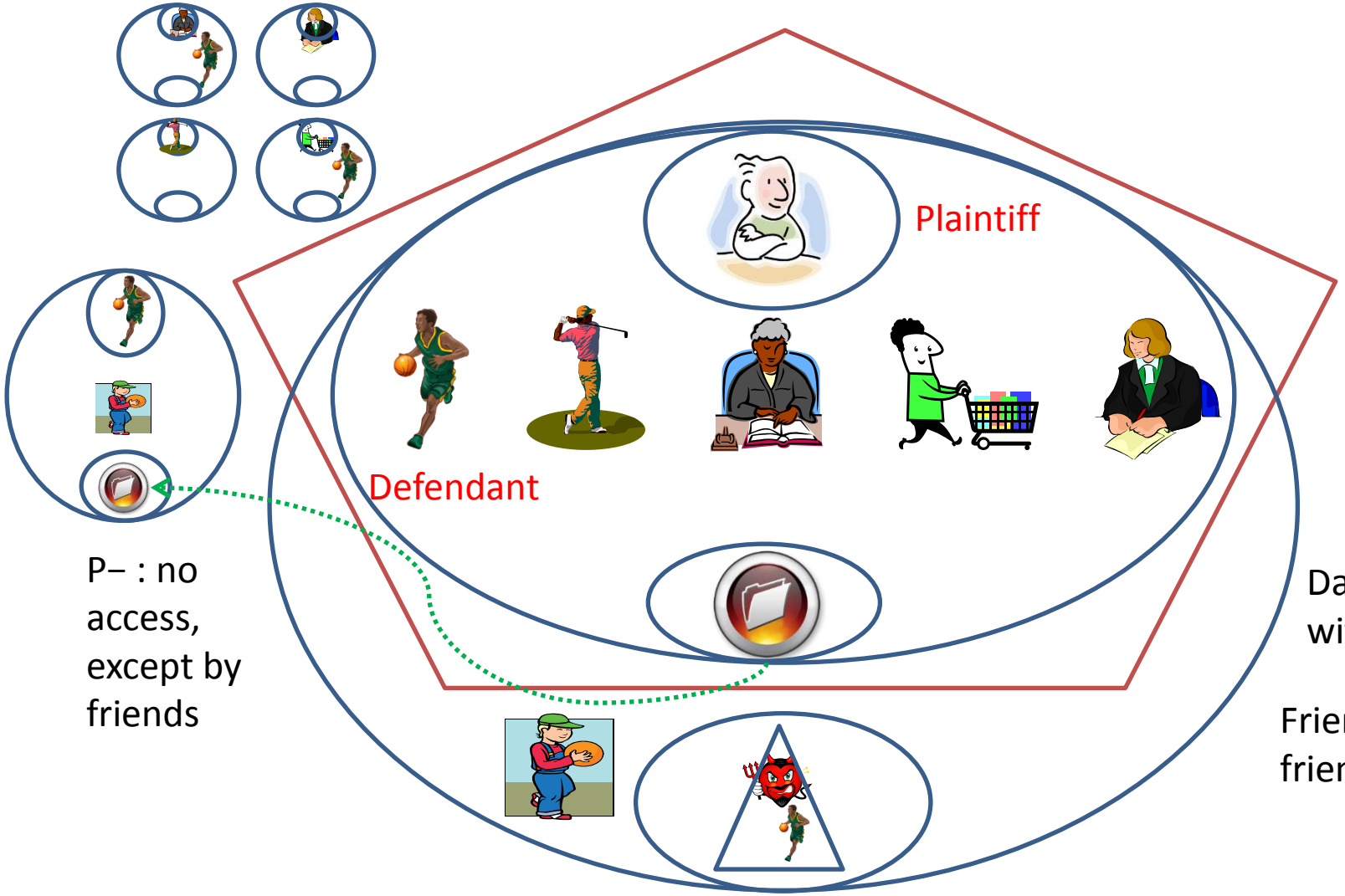
Credit Reporting Code: Requirement for Notice



Prosser's Torts

1. Intrusion upon seclusion or solitude, or into private affairs;
2. Public disclosure of embarrassing private facts;
3. Publicity which places a person in a false light in the public eye;
4. Appropriation of name or likeness.

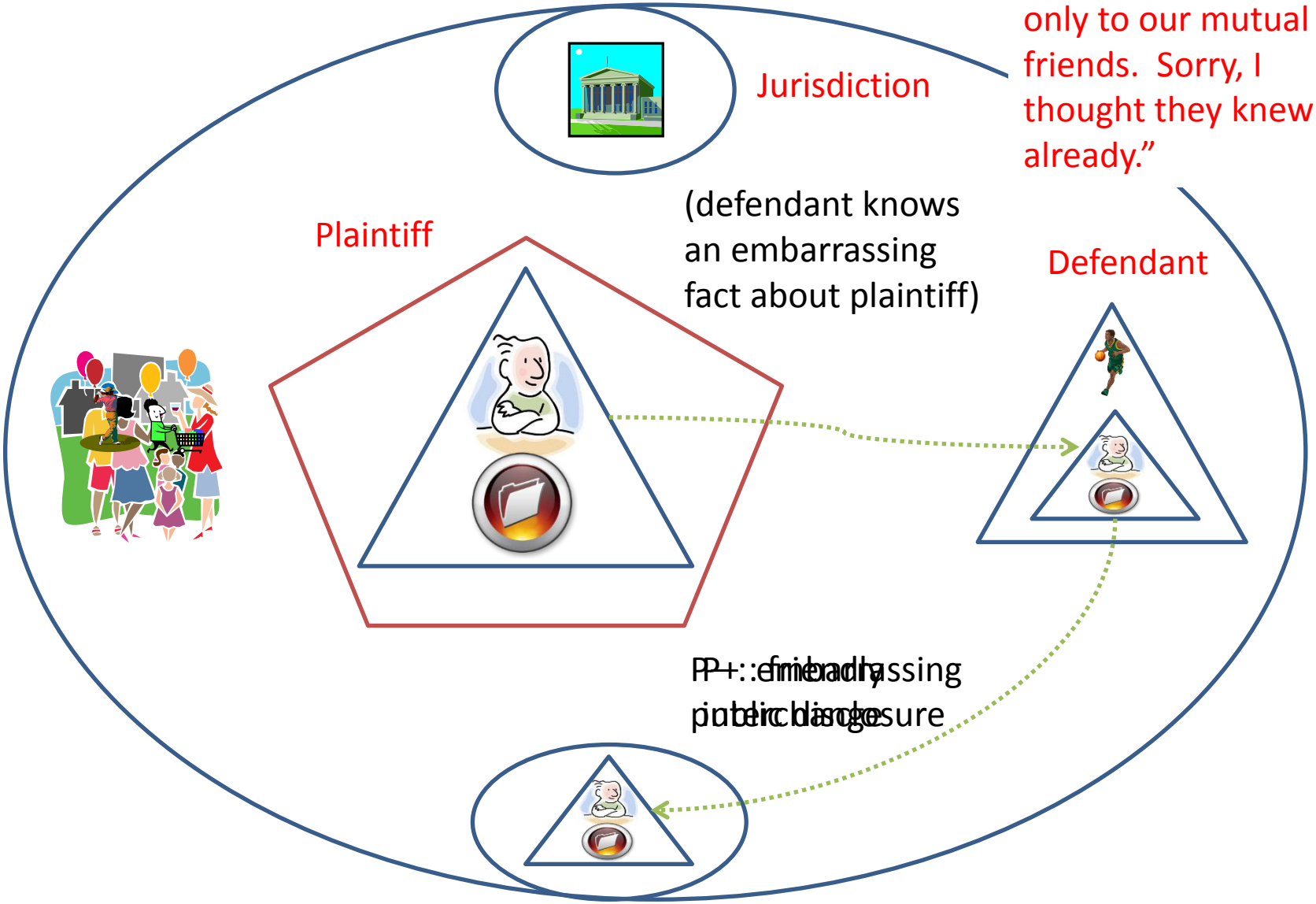
An Intrusion Into Private Affairs



Possible defence:
“Sorry, I had no idea that ‘liking’ your posting would publish it to my friends.”

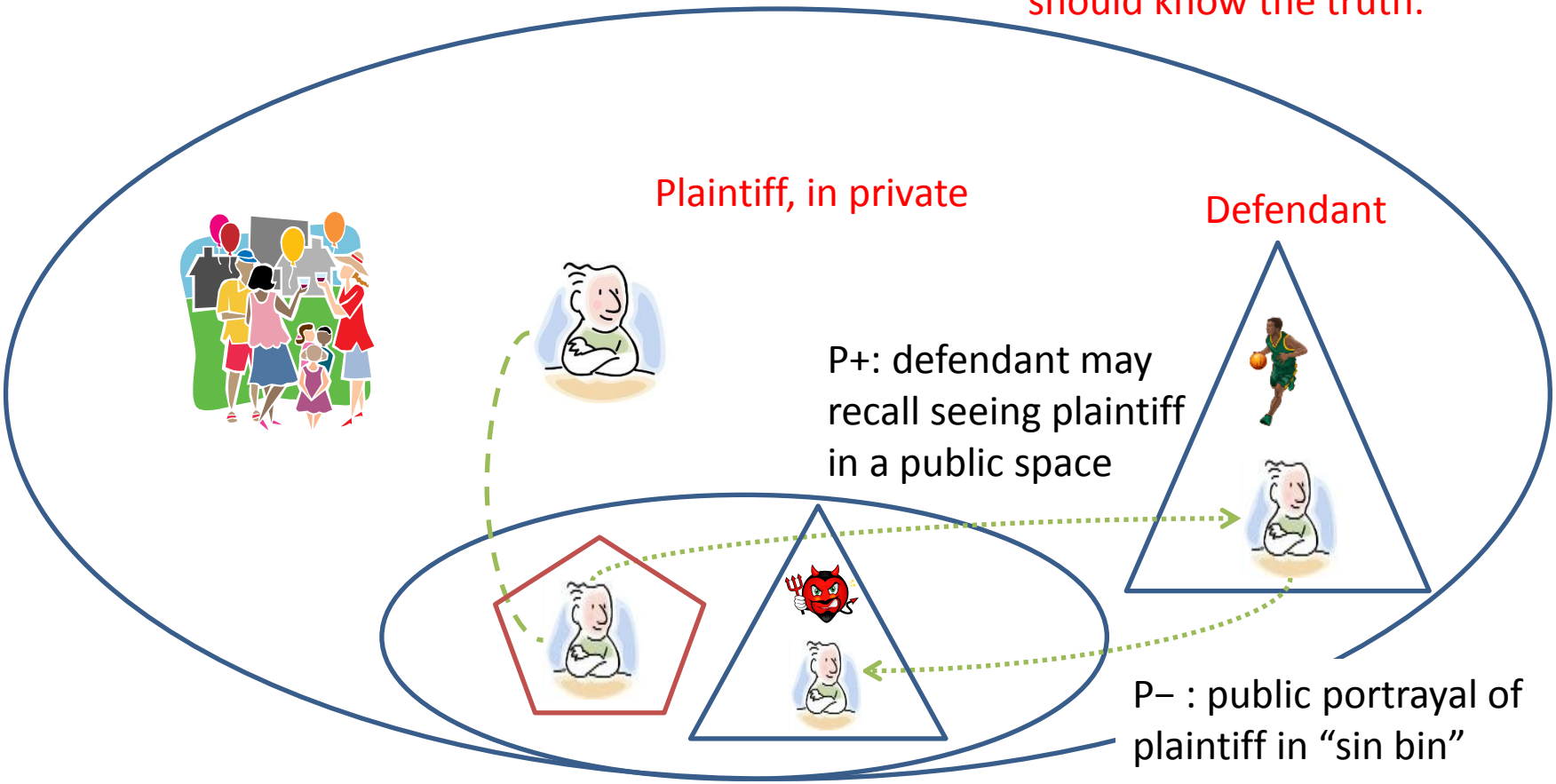
A Public Disclosure

Possible defence: "I disclosed this fact only to our mutual friends. Sorry, I thought they knew already."



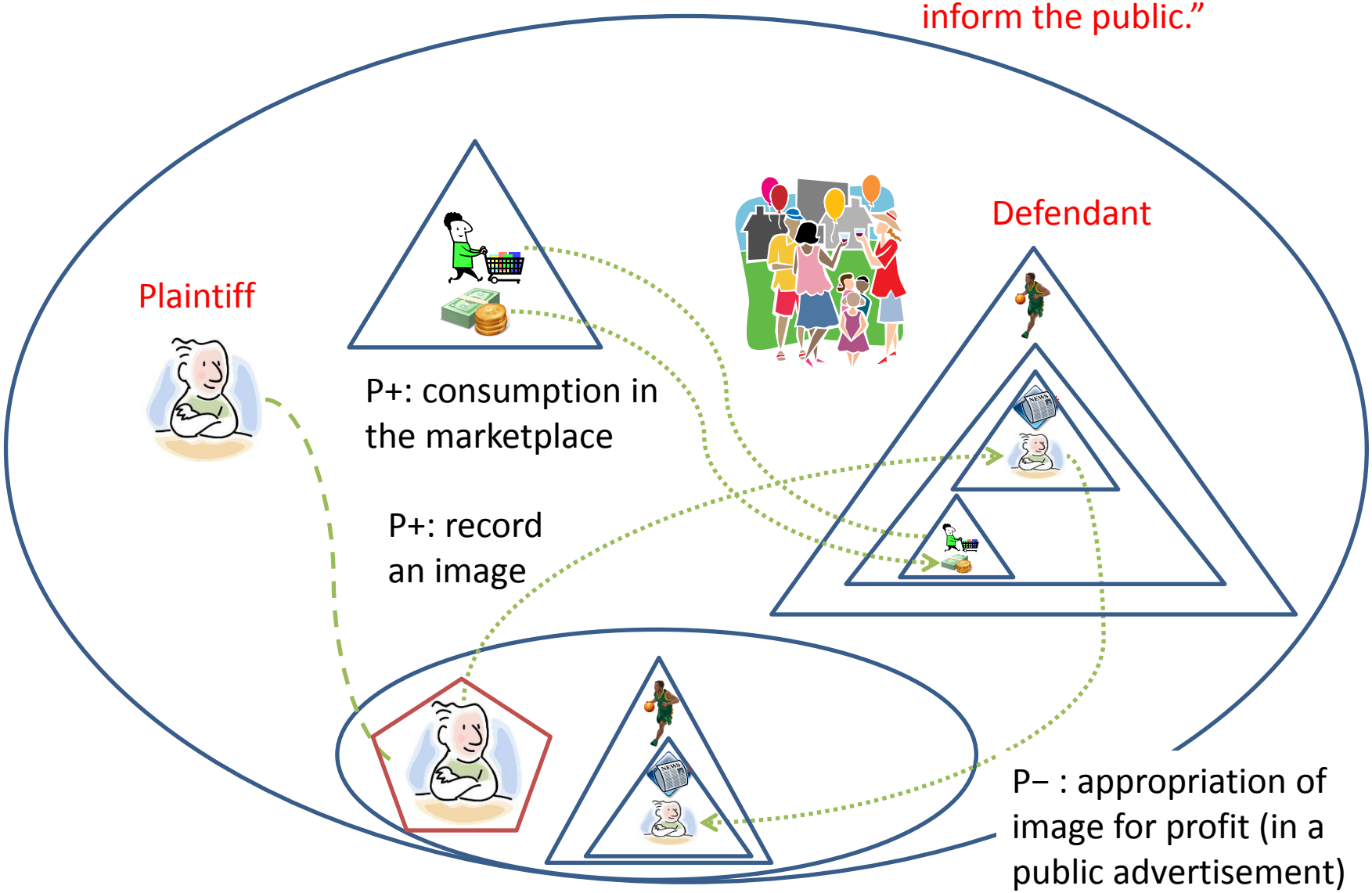
A False Light

Possible defence:
"I saw you doing that terrible thing. I think the public should know the truth."



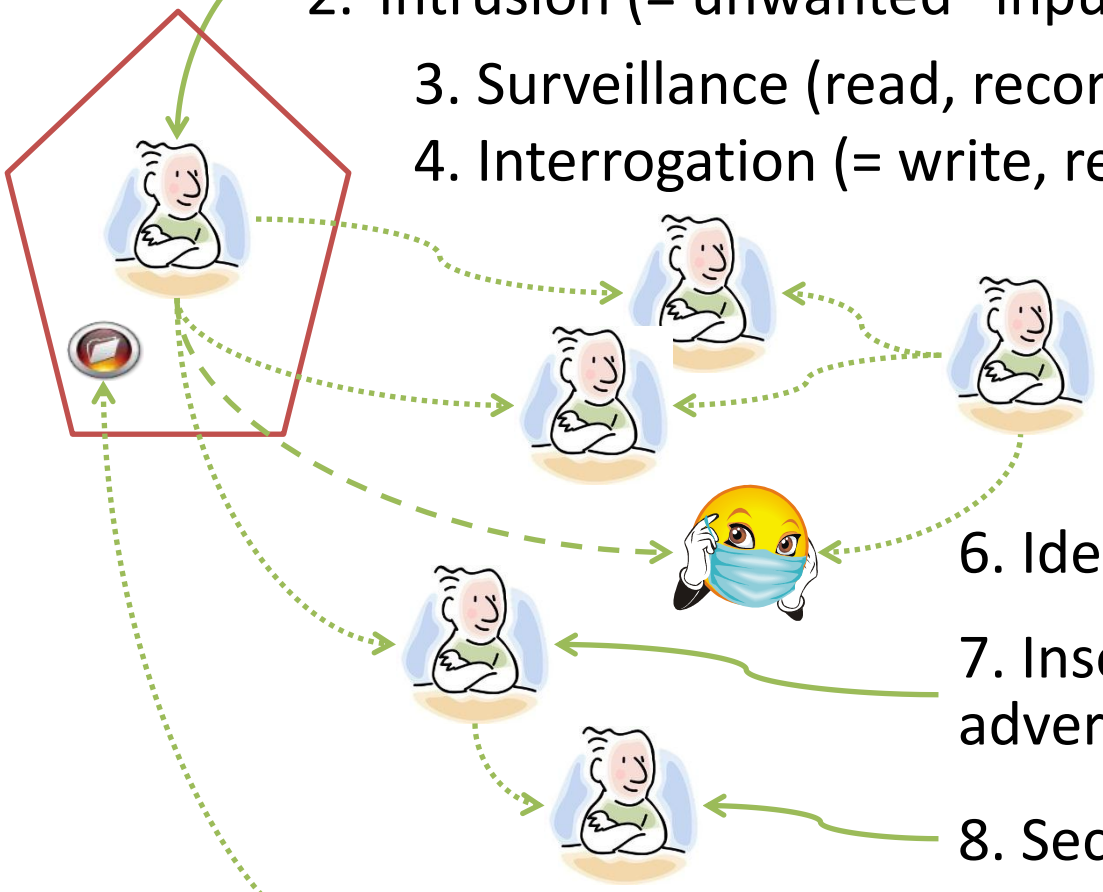
An Appropriation

Possible defence:
"I am not trying to make a profit. My motivation is to inform the public."



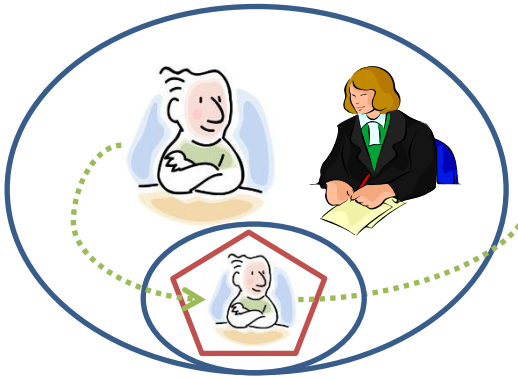
Solove's 16 Harmful Activities

1. Decisional interference (= observing some activities)
2. Intrusion (= unwanted "inputs")
3. Surveillance (read, record)
4. Interrogation (= write, read, record)



5. Aggregation (= constructing a "master copy")
6. Identification
7. Insecurity (= not preventing adversarial control)
8. Secondary use
9. Exclusion (= failing to provide adequate notice)

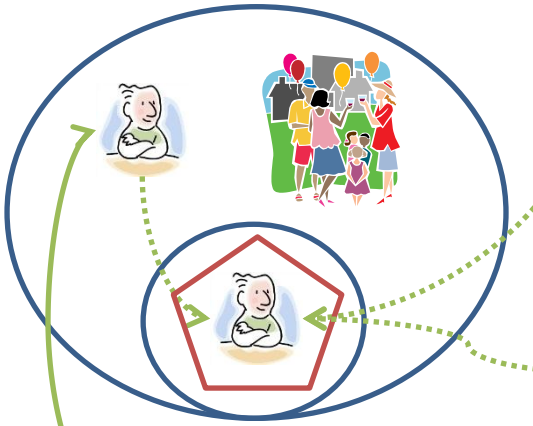
Solove's 16 Harmful Activities (cont.)



10. Breach of confidence

11. Distortion (= aggregation with inaccurate data)

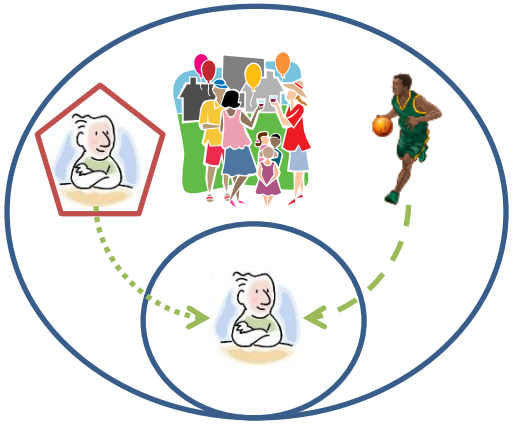
12. Disclosure (= aggregation with truthful information affecting public judgement of character, beyond "normal boundaries of information flow")



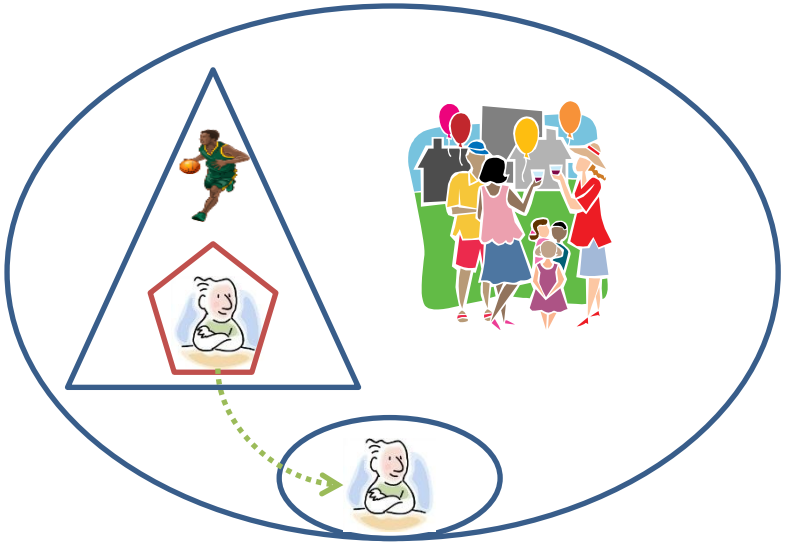
13. Exposure (= aggregation with truthful information in breach of reserve e.g. of modesty)

14. Blackmail (with a threat of information dissemination)

Solove's 16 Harmful Activities (3)



15. Appropriation (= an aggregation of someone else's image with your own persona)



16. Increased accessibility

It’s only a model…

- My model can represent the architectural aspects of privacy: “What might be controlled by a computer?”
- It could be used for the elicitation of privacy requirements: “What should be controlled?”
  - It could be used to harmonise privacy requirements (or to prove that harmonisation is infeasible).
- It could be used for the evaluation of privacy protections: “What is controlled?”
  - It could be used to explain and educate.
- Will you use it? Please let me know!