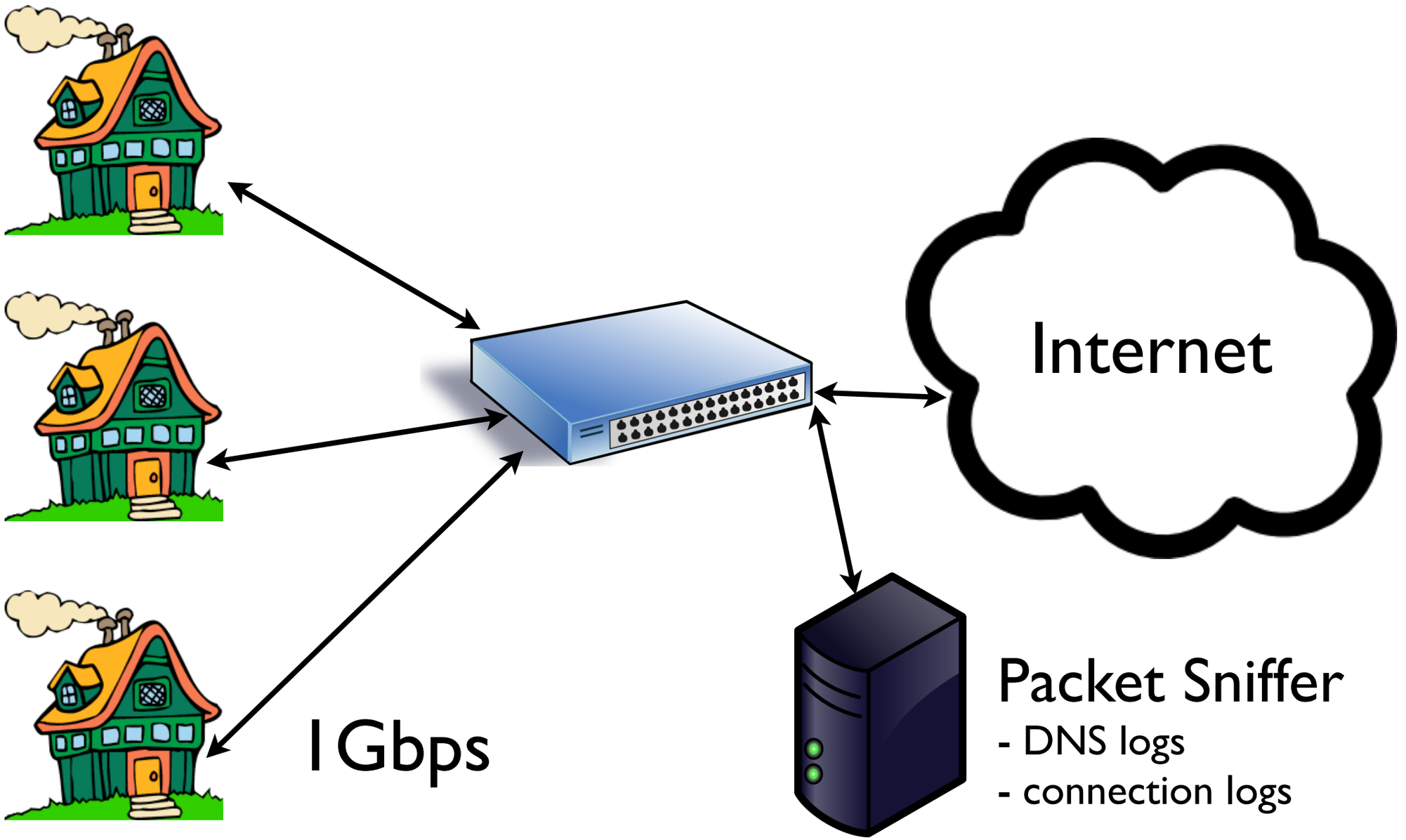
Traffic Monitoring Considered Reasonable

Mark Allman
International Computer Science Institute

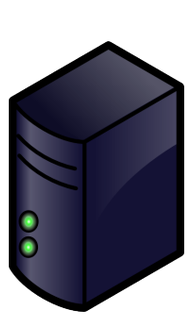
CREDS
May 23, 2013

"The night is dark, but the sidewalks bright,
And lined with the light of the livin'"

A Story, Part I



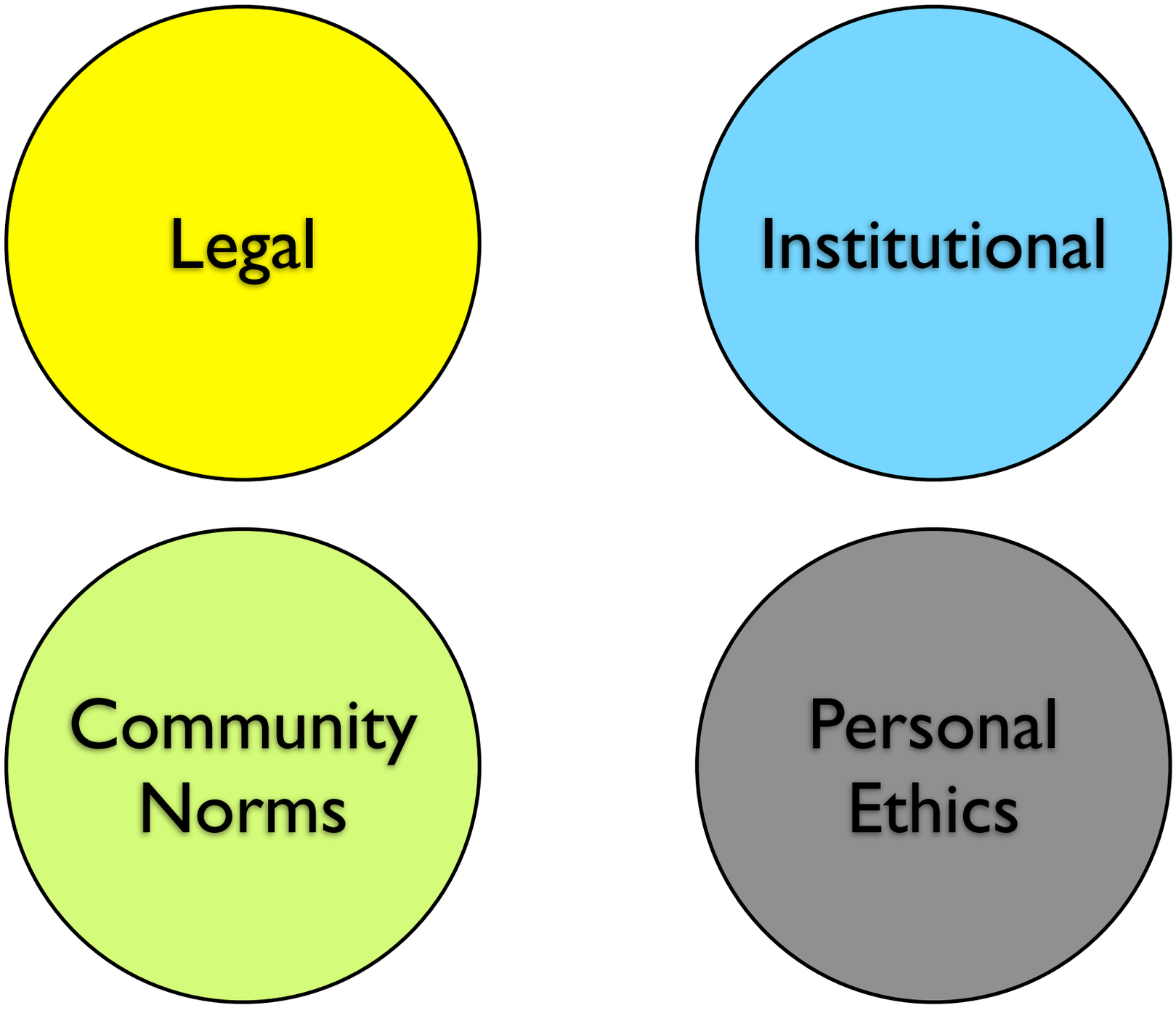
A Story, Part 2

cat  | ./  > 

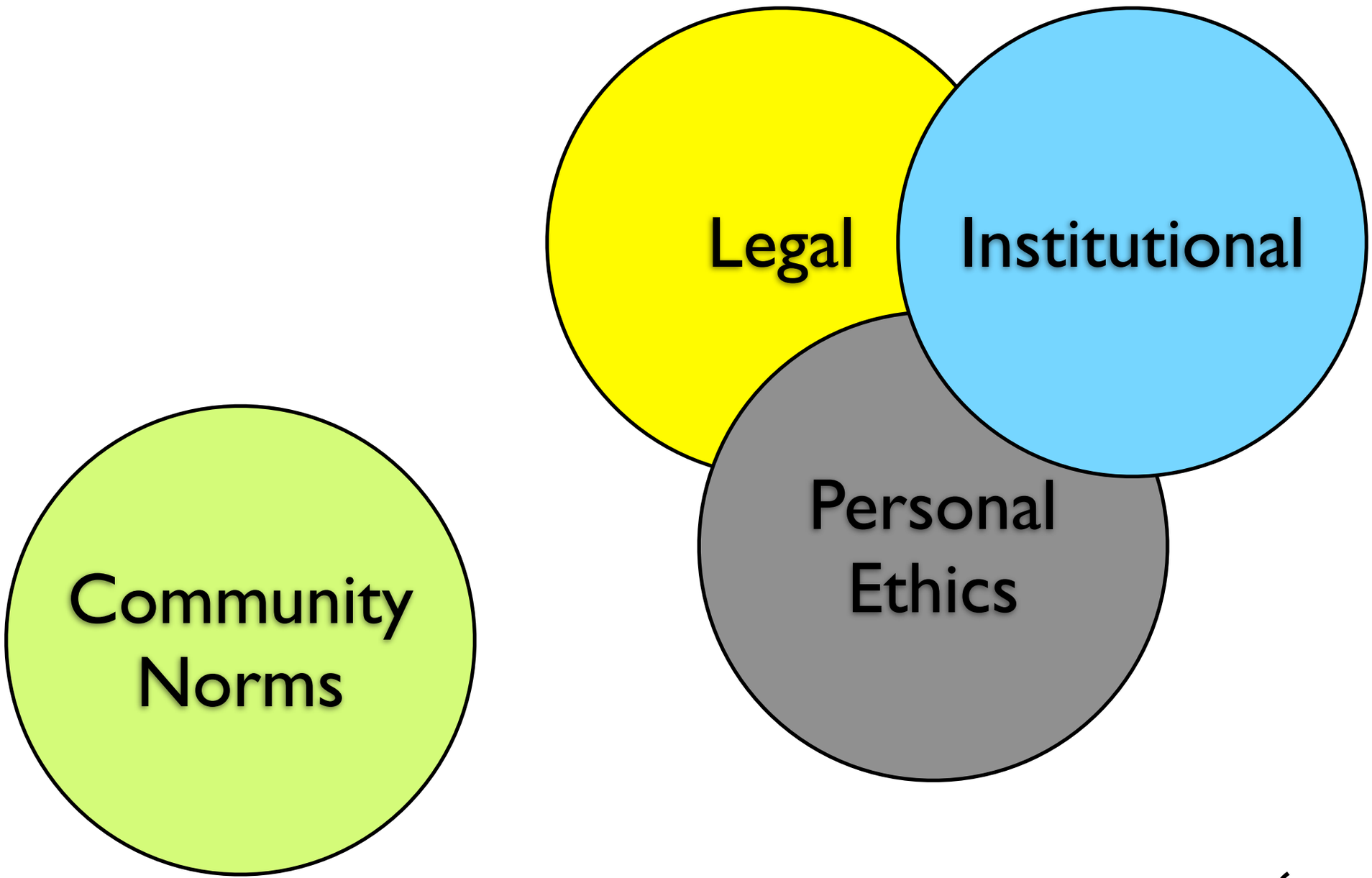
A Story, Part 3

- From a CCR review, Jan/2013:
  - *"Is there informed consent for your monitoring? What are you capturing and what are you filtering? Privacy is a huge issue, I don't think you can publish without at least explaining your methods for protecting it."*

Experimental Constraints



Experimental Constraints



Explicit Position

- *Network traffic monitoring---broadly defined---fits well within the networking and security research community's norms.*

Community History

- Community history is clear ...
  - ... much traffic monitoring
  - ... at various layers
  - ... by myriad researchers
  - ... across a breadth of time
  - ... appearing in many, many venues
  - ... vetted by thousands of people

Benefit vs. Harm

- Benefits of observing Internet operation *in the wild* are clear
- But, what about harms?
  - we can dream of *potential* dire consequences
    - ... usually some form of painful death!
    - ... of a child!
  - but, we have a pretty good track record of very few *actual* harms

Conclusion

- The community has *rough consensus and running code* that traffic monitoring is reasonable

- Therefore, *the presumption should be that investigations that observe it-situ activities should be considered well within the bounds of what the community considers to be reasonable.*

Implicit Position

- We should start stating the norms that have developed organically
- But, how to do this authoritatively?

INTERNATIONAL
COMPUTER SCIENCE
INSTITUTE

Questions? Comments?

Mark Allman

mallman@icir.org
http://www.icir.org/mallman/