UNIVERSITY of TORONTO

Analyzing Trust in Technology Strategies

Privacy, Security, Trust 2006
Markham, Ontario, Canada
October 31, 2006

Jennifer Horkoff
Department of Computer Science,
University of Toronto
jenhork @ cs.utoronto.ca

Eric Yu
Faculty of Information Studies,
University of Toronto,
yu @ fis.utoronto.ca

Lin Liu
School of Software,
Tsinghua University, Beijing
linliu @ tsinghua.edu.cn

How do we develop technology strategies within a strategic business network?

I want to profit from Technology.

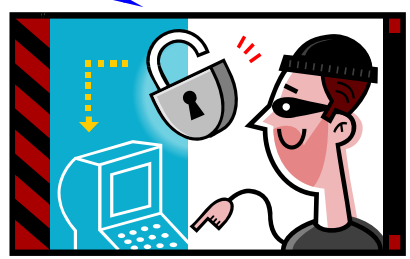
I want to acquire Technology as cheaply as possible.

I want to profit from Copyrighted Content.

I want to profit by gaining access to Technology.

I want to exchange Pirated Content!

I want to acquire Copyrighted Content as cheaply as possible.

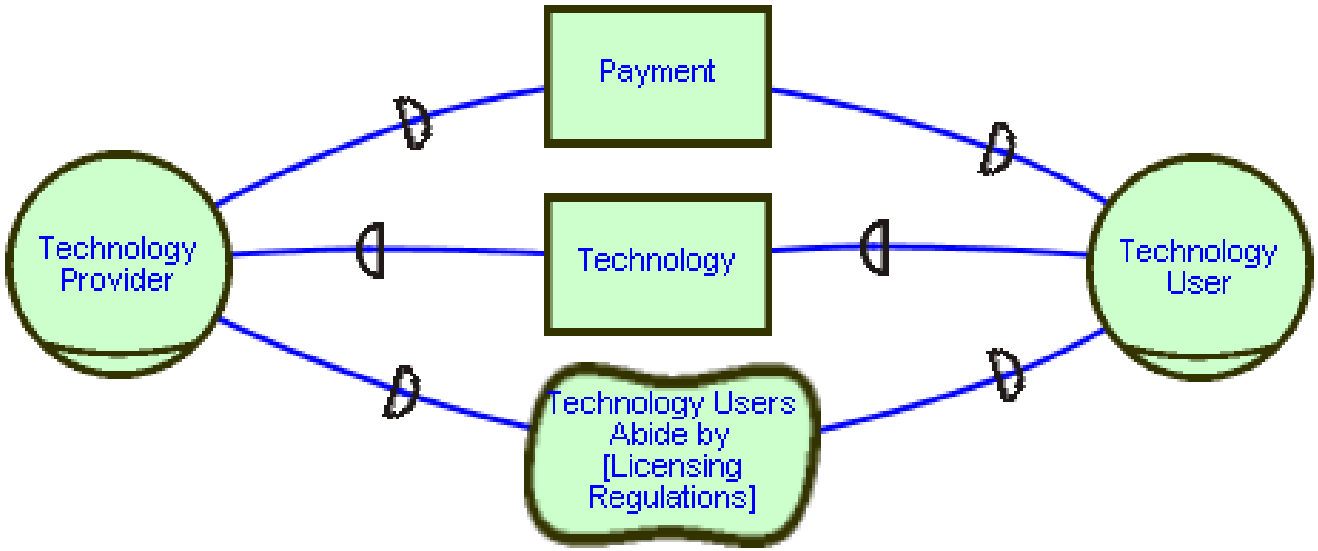


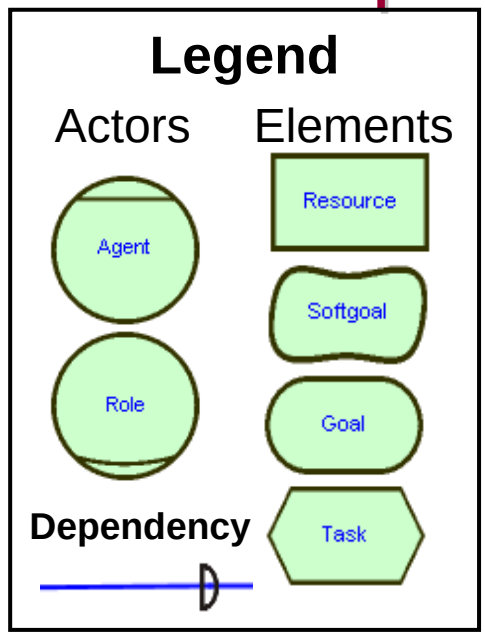
Presentation Outline

- Motivation: Understanding Technology Strategies in a Strategic Network
- Our Approach
  - Social, Intentional Modeling
  - The i* Framework
  - i* Evaluation Procedure
- Case Study: Trusted Computing
  - The Business of Content and Technology
  - Proponents of Trusted Computing
  - Opponents of Trusted Computing
- Conclusions
- Limitations and Future Work

The i* Framework

Technology User – Provider: Simplified Example

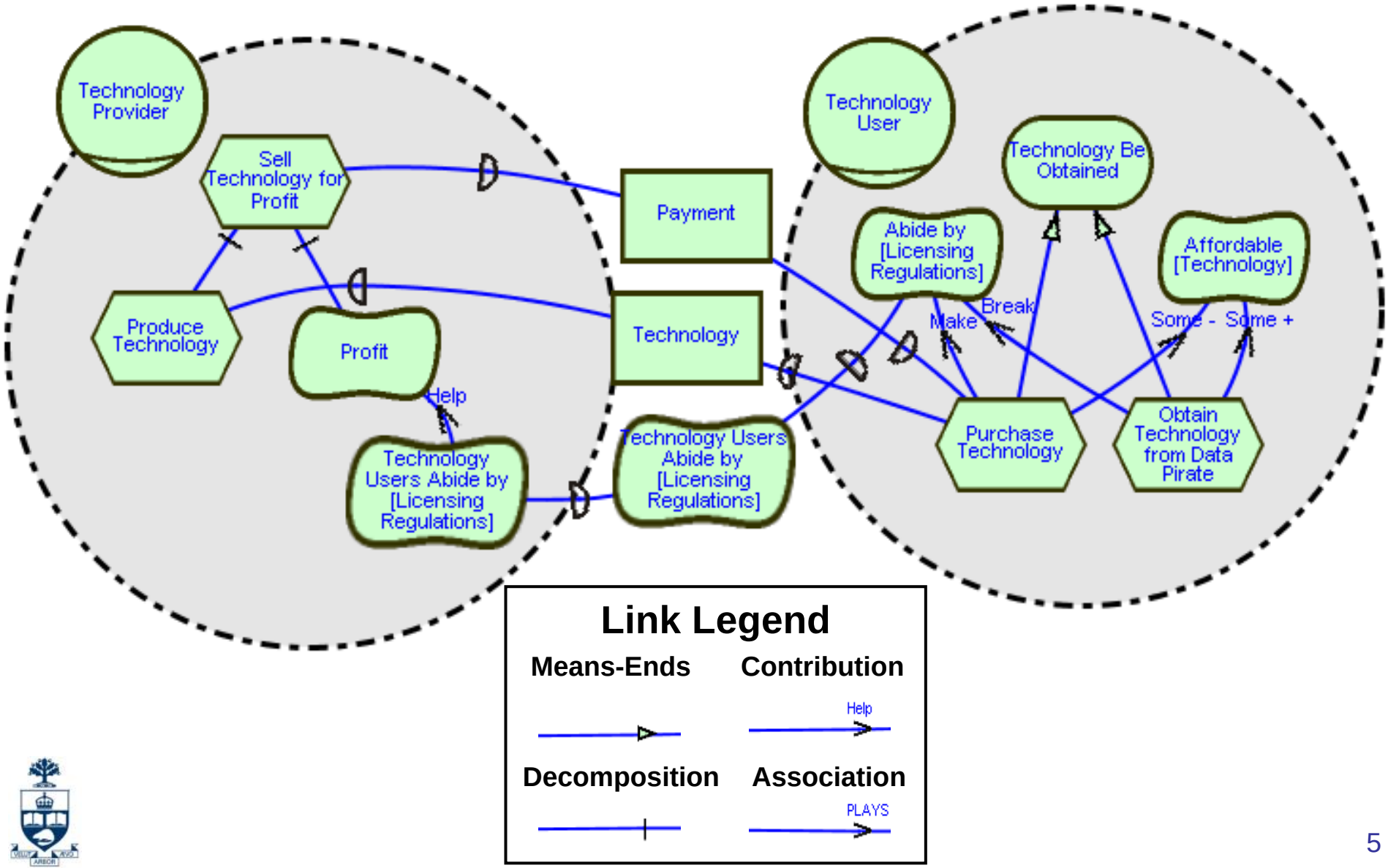




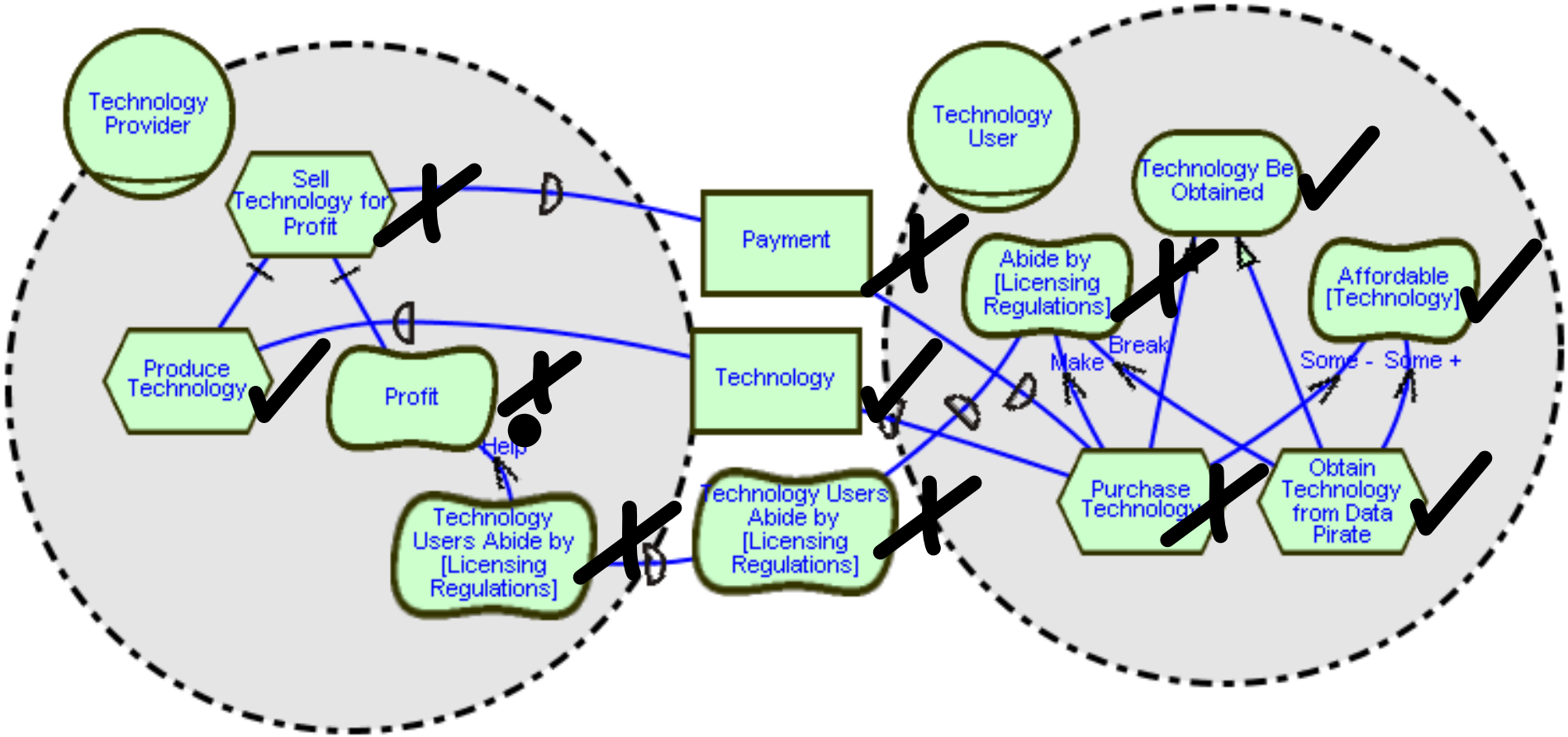
- i* uses intentional, autonomous actors
- Captures the dependencies between strategic actors
- Focuses on answering questions such as "why?", "who?", "how?", and "how else?"

The i* Framework

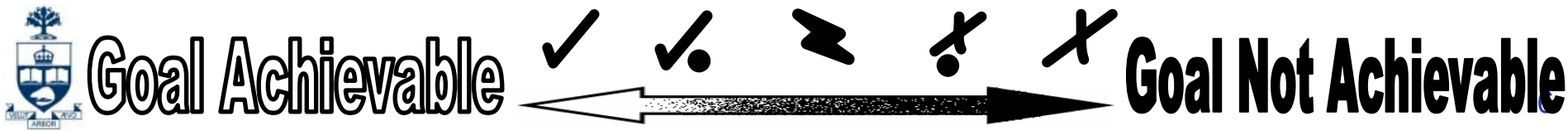
Technology User – Provider: Simplified Example



i* Evaluation Procedure

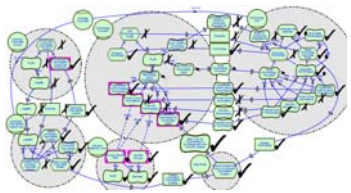


- Semi-automatable propagation of qualitative evaluation labels uses evaluation guidelines and human judgment.



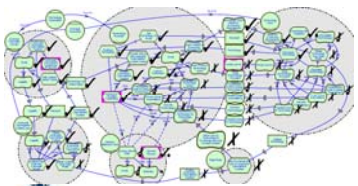
Case Study: Trusted Computing (TC)

- TC is Technology proposed by a set of technology vendors, now represented by the Trusted Computing Group (TCG).
- Case Study Steps:



- Model TC context: the business of content and technology

- Model the affects of TC according to proponents

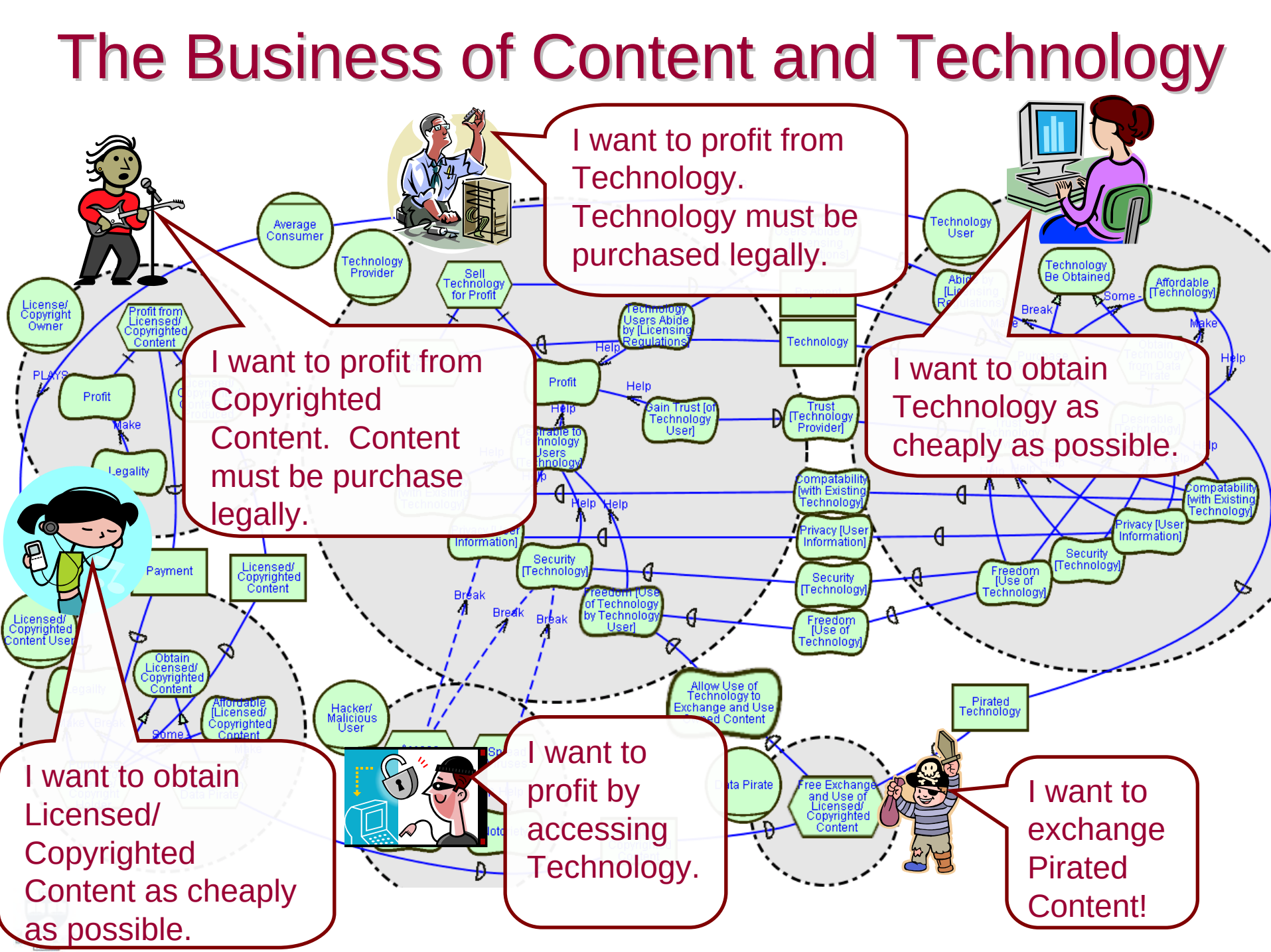


- Model the affects of TC according to opponents

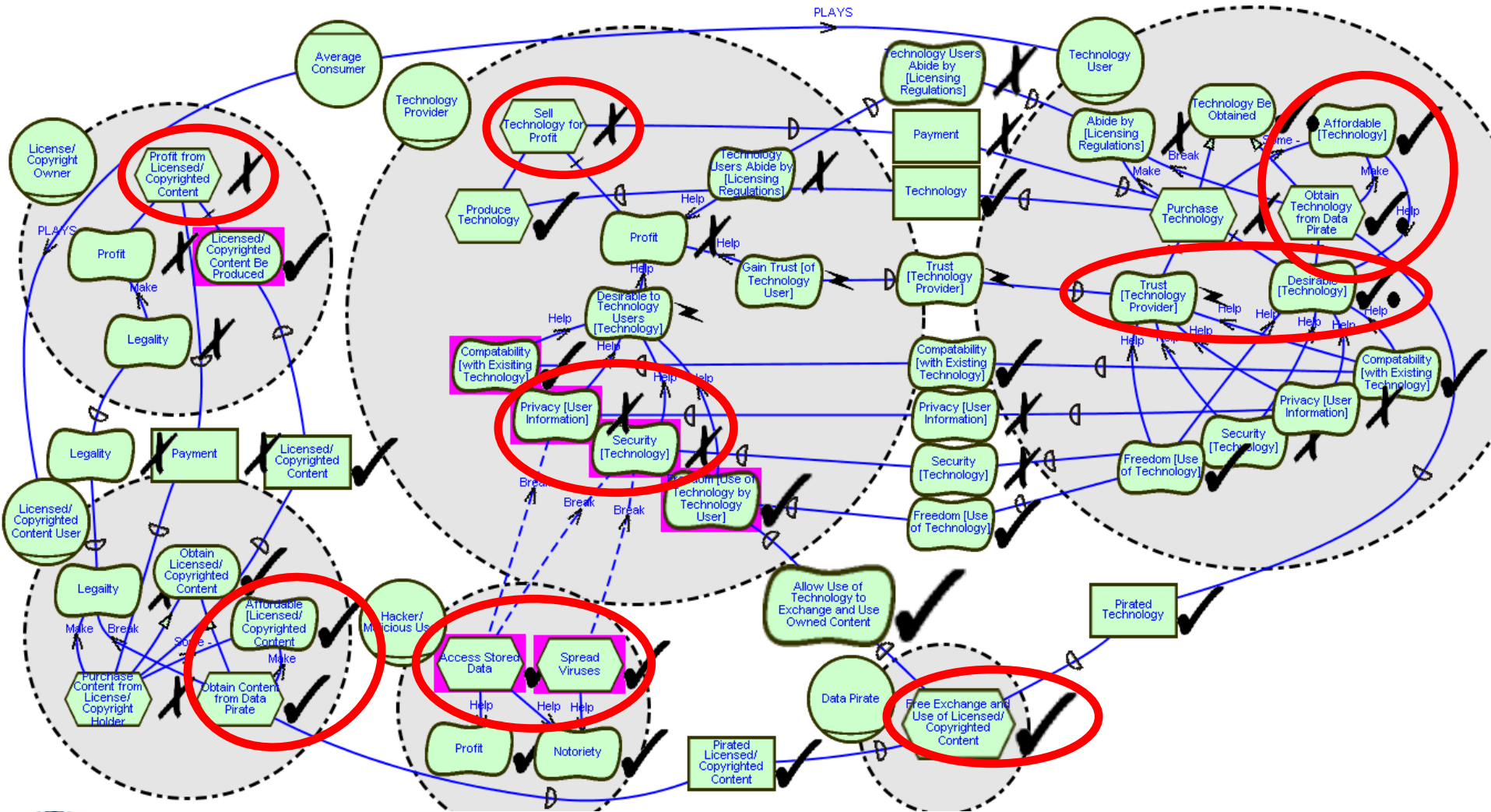
Case Study Sources

- Proponents: technical reports and FAQs of the TCG or TCG members.
- Opponents: an FAQ written by Anderson.
- All sources accessed in 2003 and 2004.

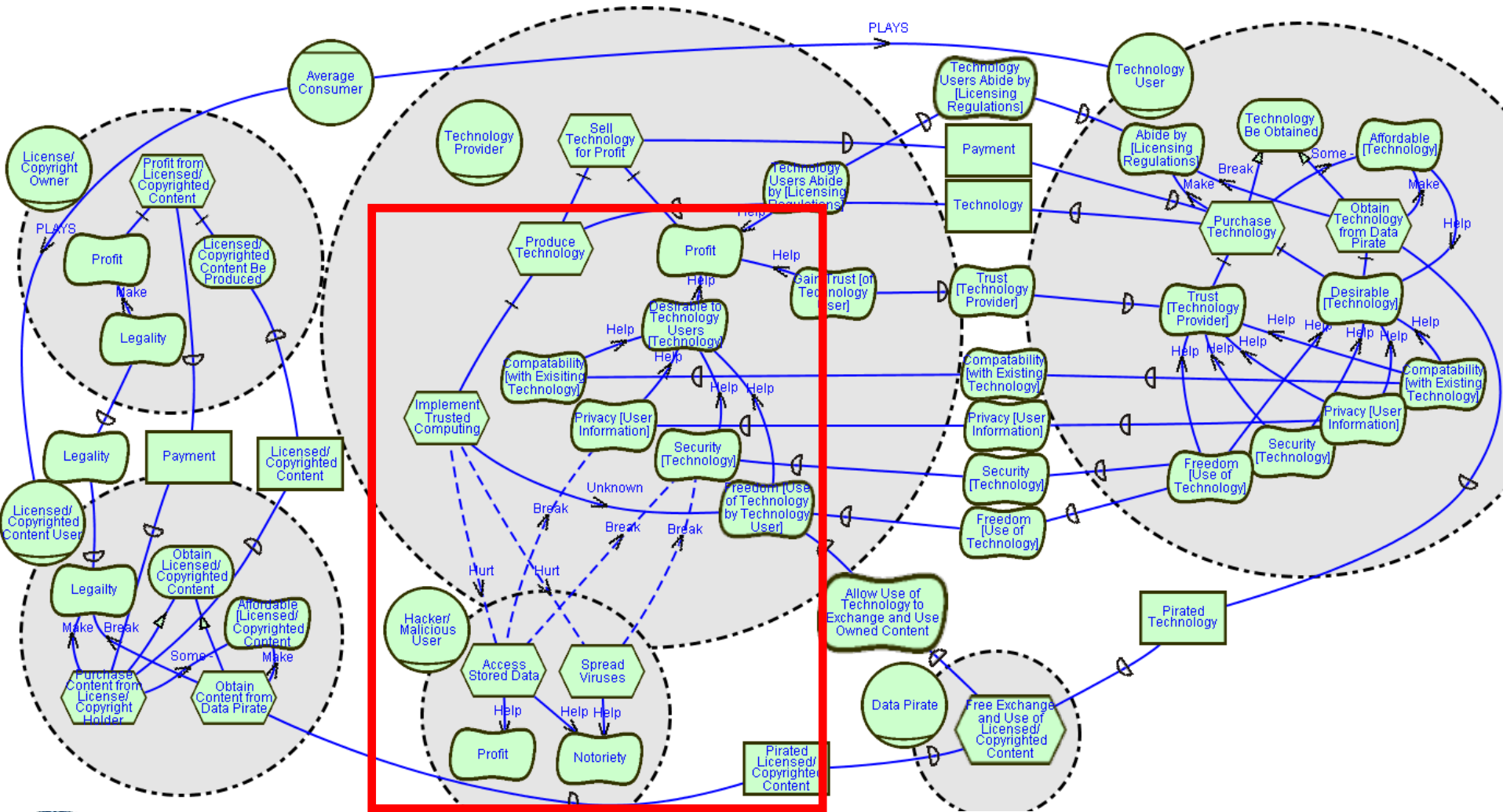
The Business of Content and Technology



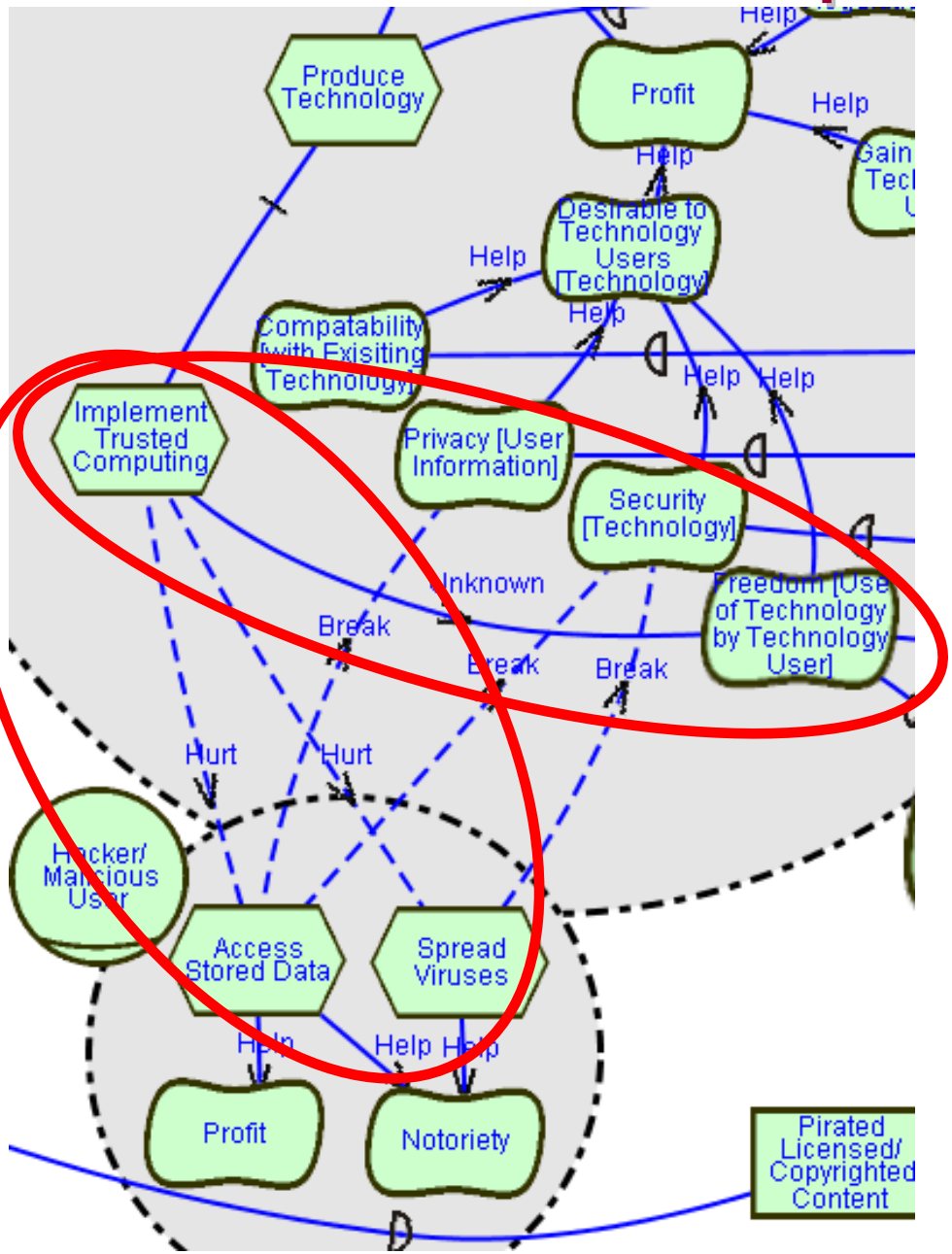
What can Evaluation reveal about this Situation?



Proponents of TC

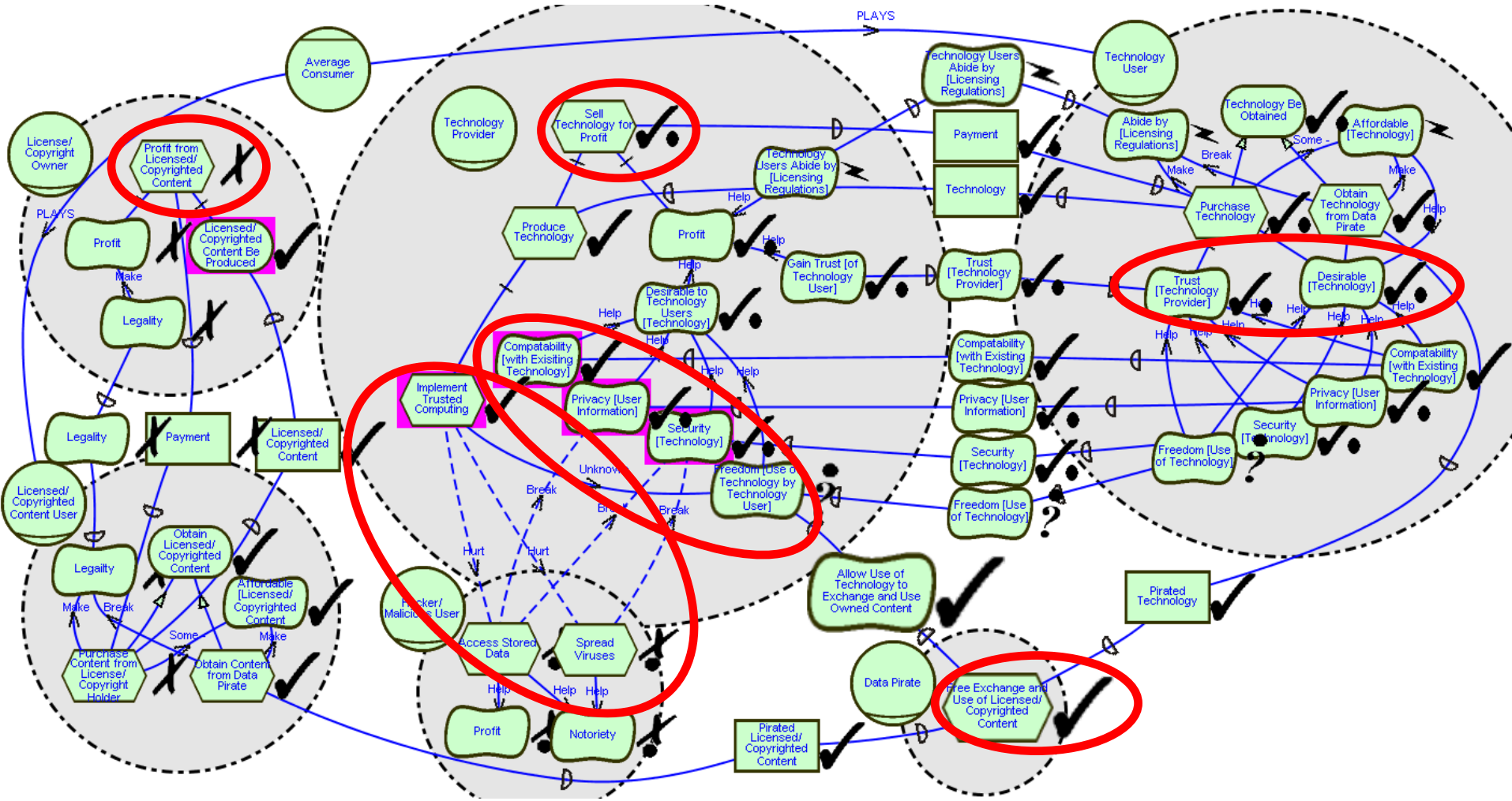


How can TC Help?

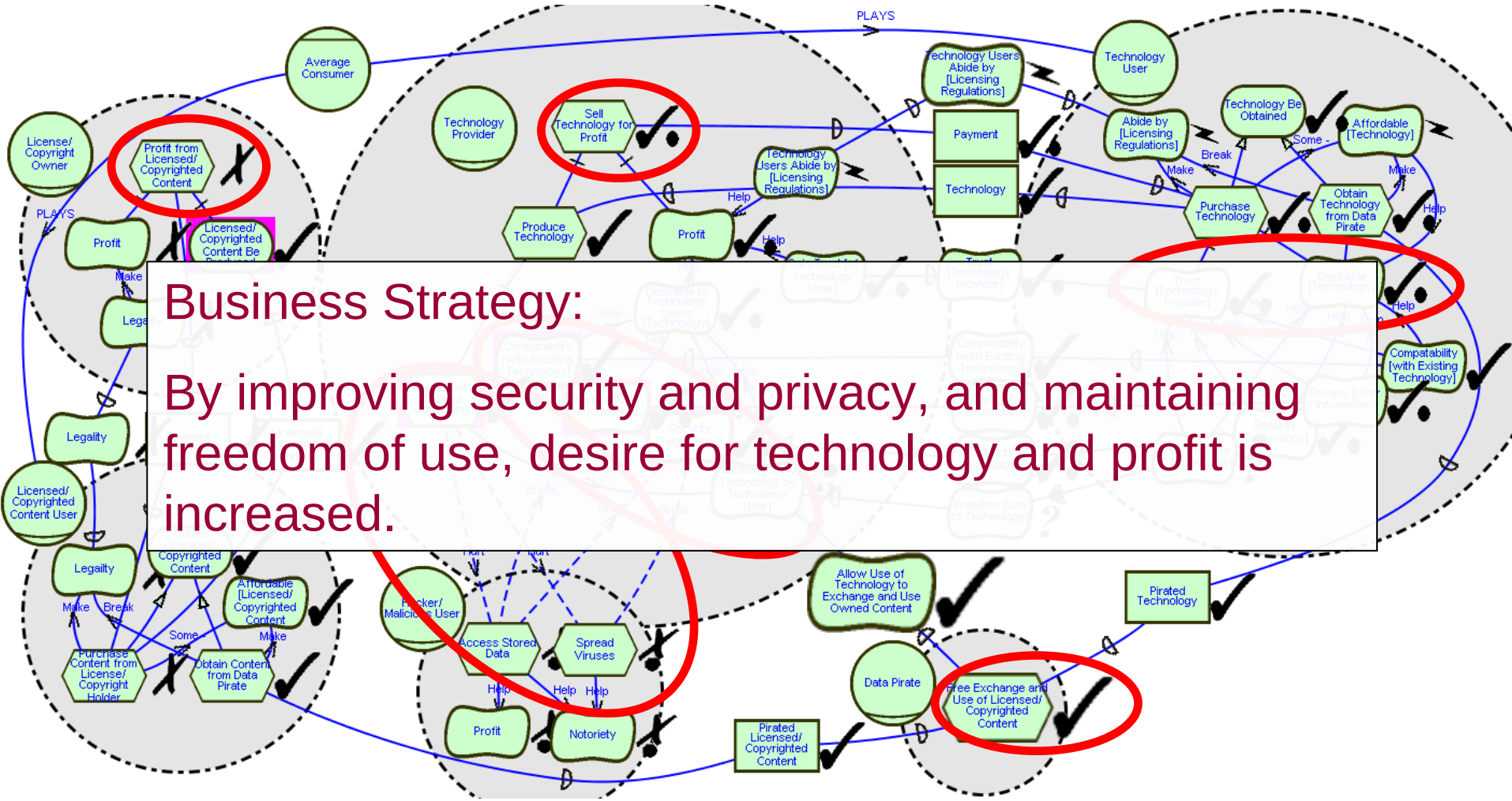


UNIVERSITY of TORONTO

Will TC Work?



Will TC Work?

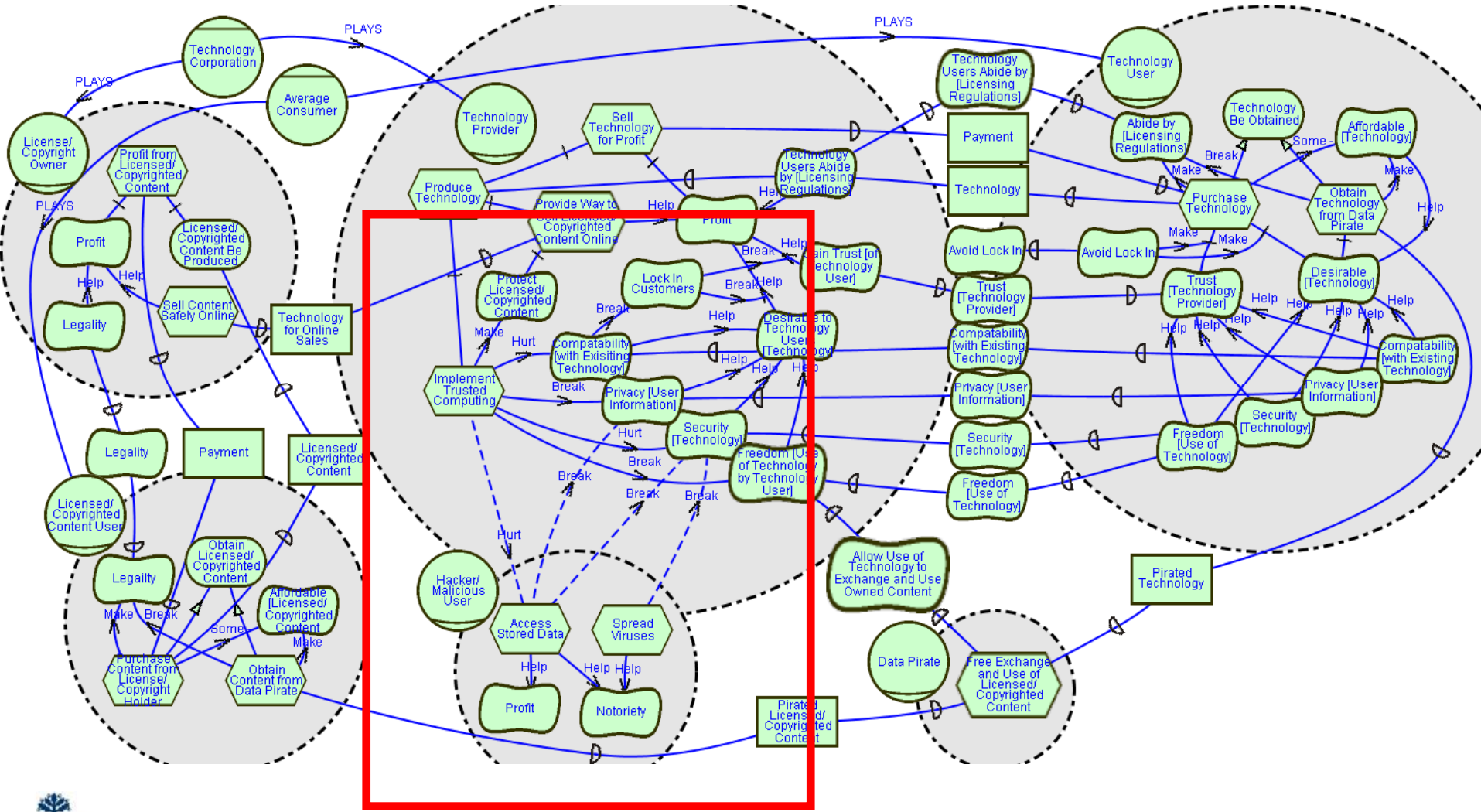


Business Strategy:

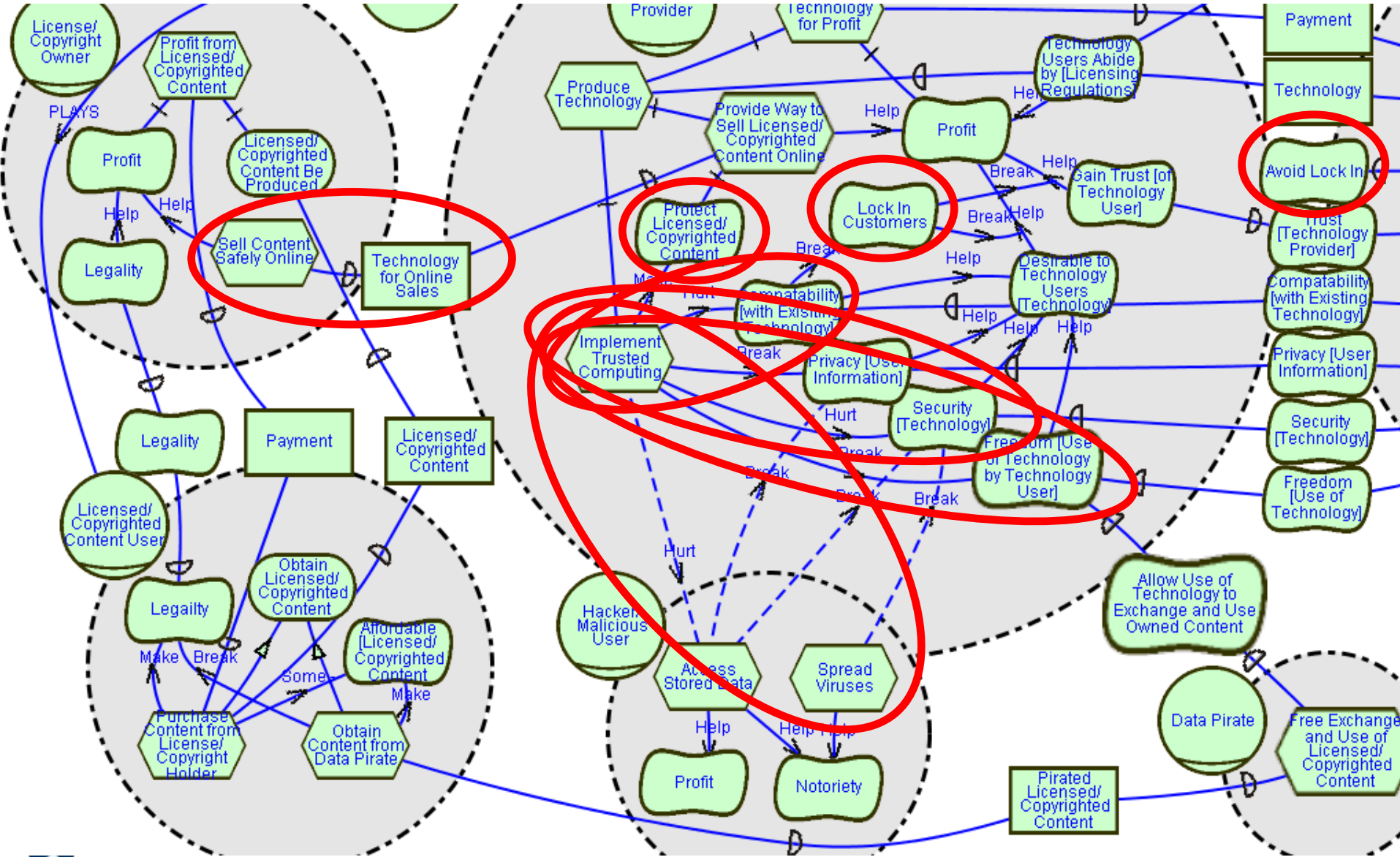
By improving security and privacy, and maintaining freedom of use, desire for technology and profit is increased.

UNIVERSITY of TORONTO

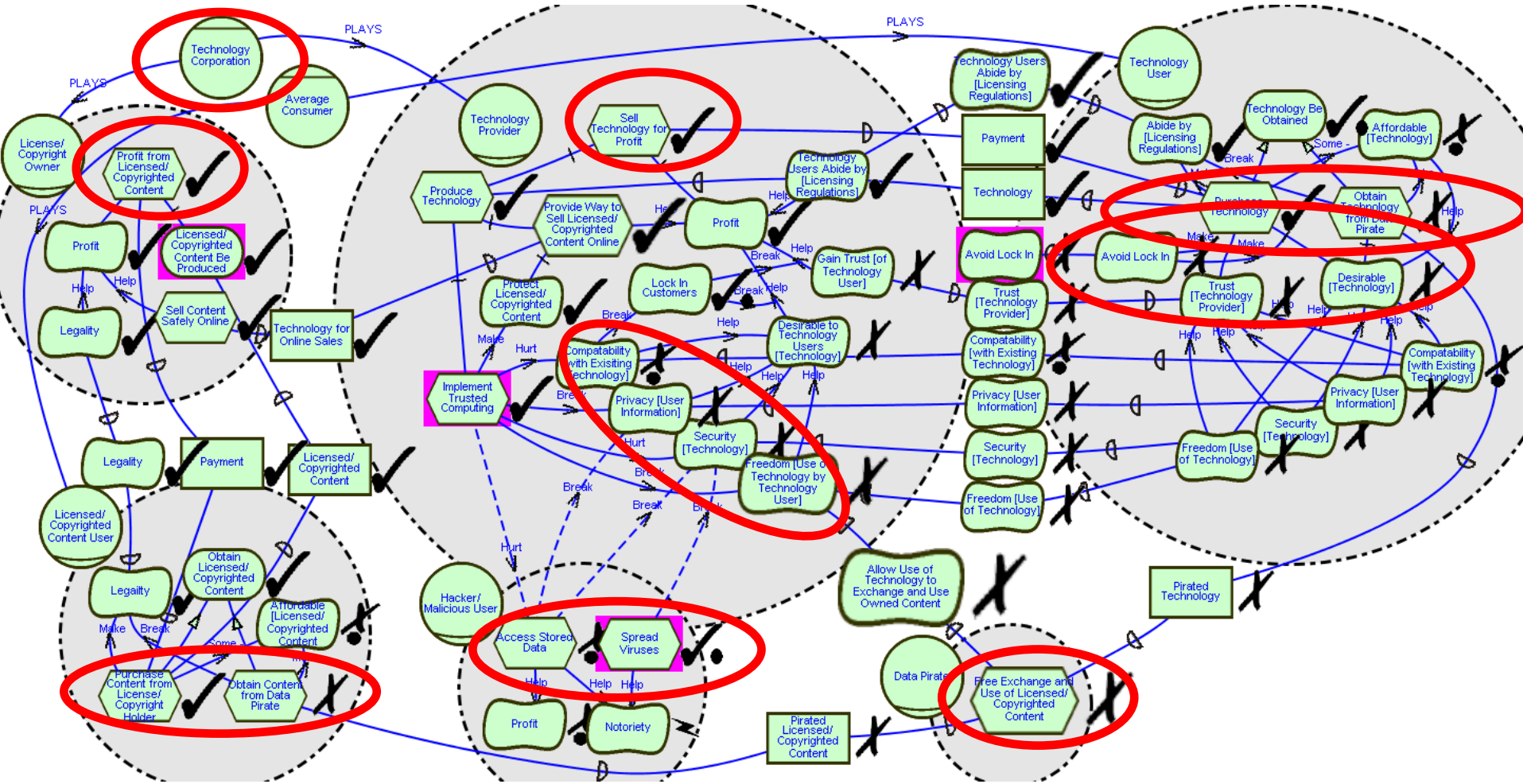
Opponents of TC



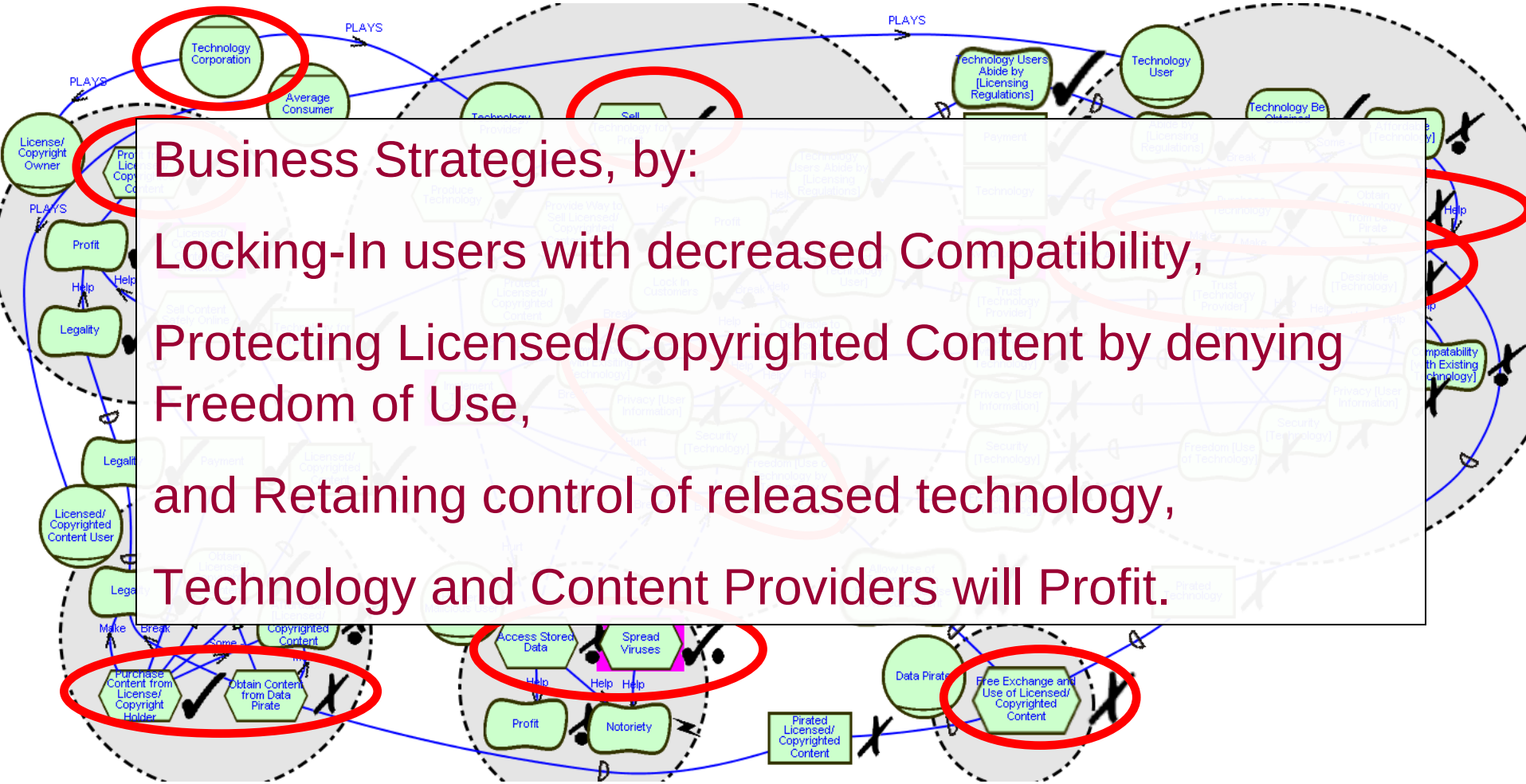
What does TC do?



How does TC Affect the Strategic Network?



How does TC Affect the Strategic Network?



Business Strategies, by:

Locking-In users with decreased Compatibility,

Protecting Licensed/Copyrighted Content by denying Freedom of Use,

and Retaining control of released technology,

Technology and Content Providers will Profit.

Conclusions

- Intentional, social, conceptual modeling depicts the links between business strategy and technology implementations.
- This type of modeling allows impact analysis – answering “What if?”, “Why?”, “How?”, provoking an inquiry cycle.
- Modeling intentions allows the explicit depiction of conflicts between viewpoints.

Case Study Insights

- Modeling revealed results which were not otherwise obvious.
  - In the first version of the opponent model we asked: "Why would the Technology Producer implement TC when it makes technology less desirable for consumers?"
    - Further iterations showed that lock-in and DRM make it worthwhile
- Gaps or flaws in arguments became more apparent when modeled:
  - Does making Technology more desirable really reduce Piracy? (proponent model)
    - If not, how will the Technology Producer benefit from TC?

Related Work

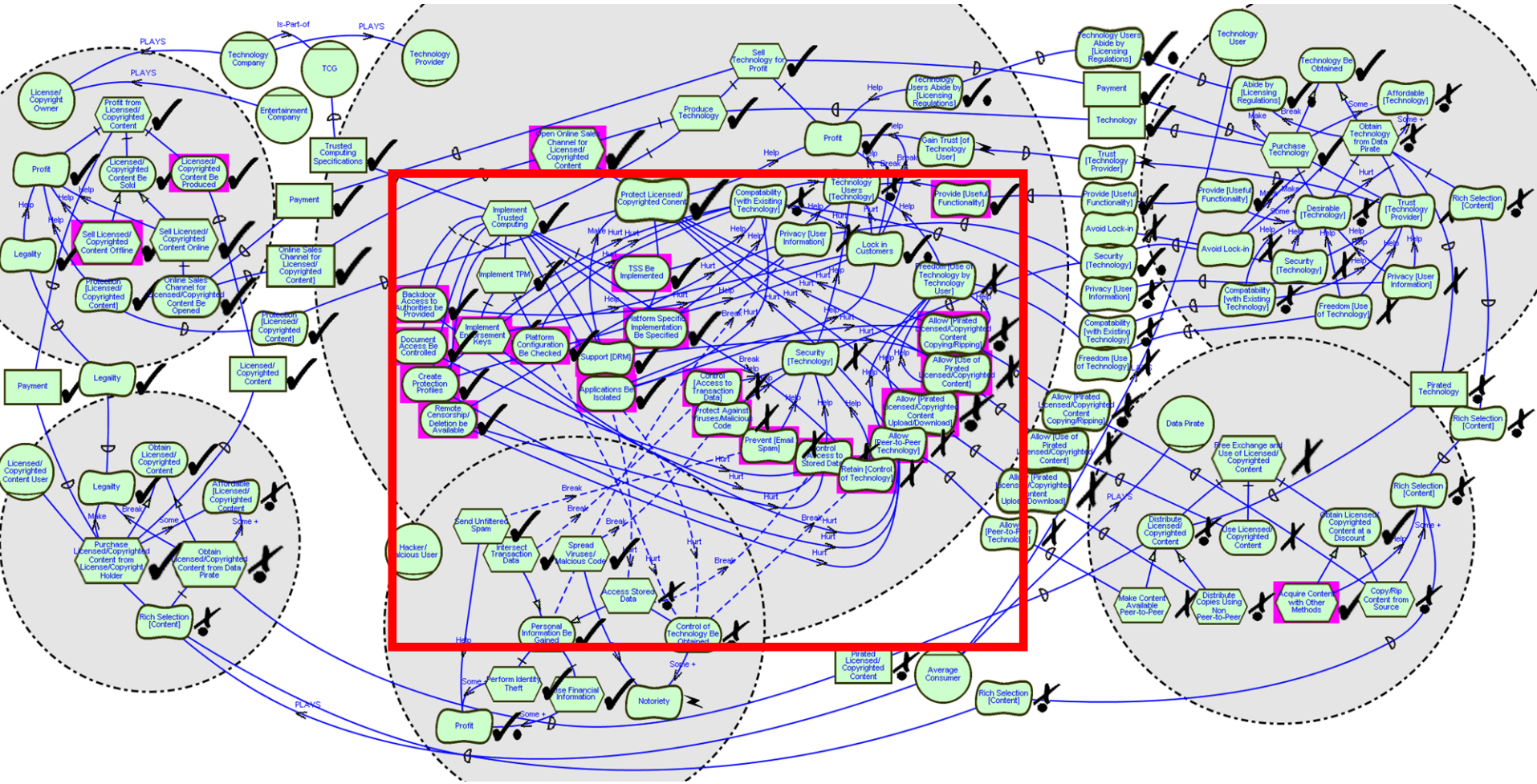
- We treat Trust as a softgoal, a qualitative goal without clear-cut criteria for success.
- This perception of trust in this work differs from previous work that treats trust as a measurable quantitative probability [Gambetta (ed.)] [Falcone, Tan (eds.)]
- In the Trust-Confidence-Distrust (TCD) Trust is represented in i* models using quantitative utility functions. [Gans et al.]

Limitations and Future Work

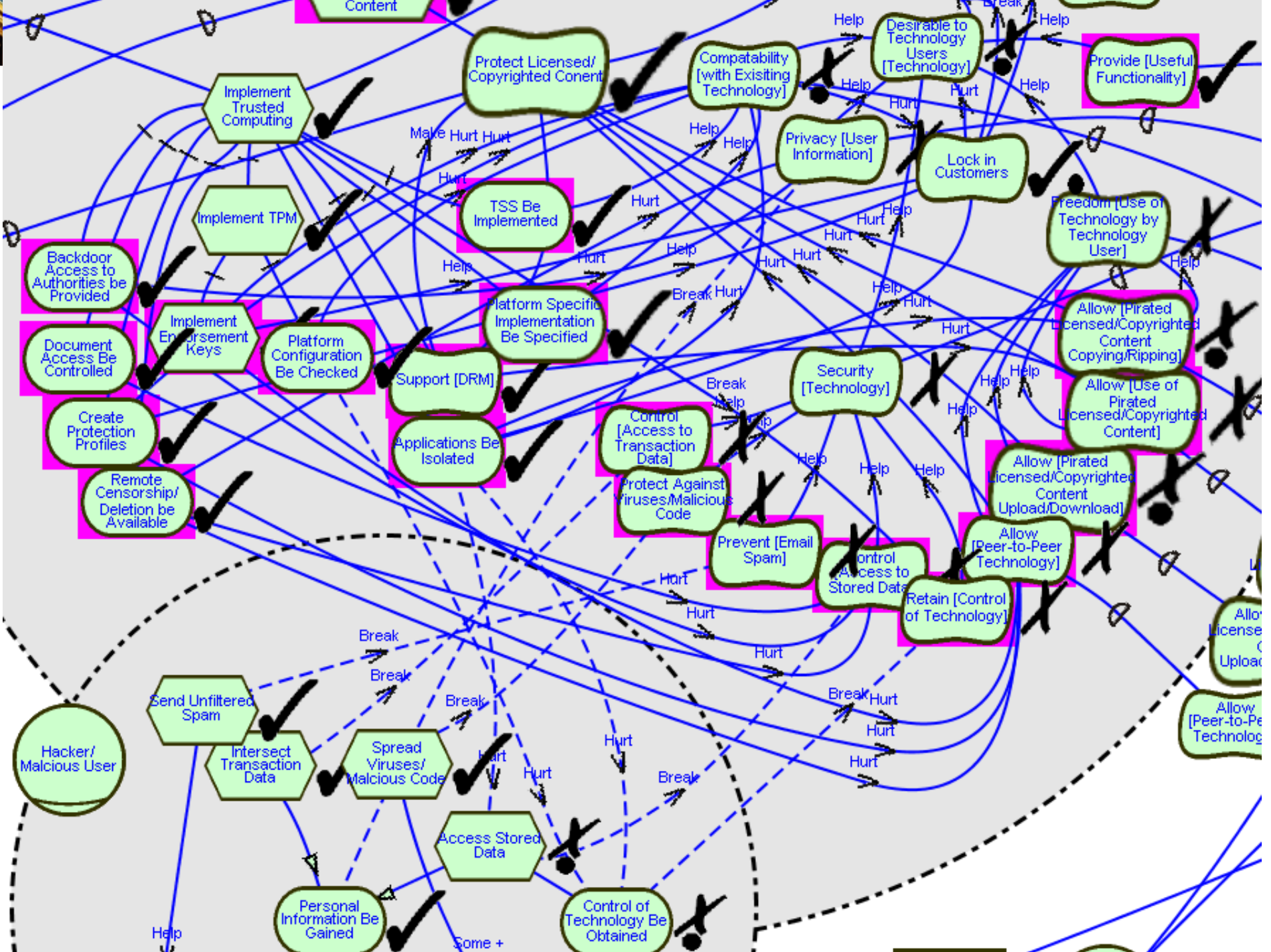
- Limitations:
  - Multiple sources combined together into only two viewpoints.
  - Does not fully explore the complex relationships between privacy, security and trust.
  - High-level, conceptual models are never fully complete or accurate.
  - Some elements are derived by the subjective interpretation of the modeler.

- Future Work:
  - Guidelines for methodology.
  - Scalability and “presentability” of i* models.

TC Opposition: Example Detailed Model



- Example: Scalability Issues


Content
Protect Licensed/ Copyrighted Conent
Compatability [with Exisiting Technology]
Desirable to Technology Users [Technology]
Provide [Useful Functionality]
Implement Trusted Computing
Privacy [User Information]
Lock in Customers
Implement TPM
TSS Be Implemented
Freedom [Use of Technology by Technology User]
Backdoor Access to Authorities be Provided
Platform Specific Implementation Be Specified
Allow [Pirated Licensed/Copyrighted Content Copying/Ripping]
Implement Endorsement Keys
Platform Configuration Be Checked
Document Access Be Controlled
Support [DRM]
Security [Technology]
Allow [Use of Pirated Licensed/Copyrighted Content]
Create Protection Profiles
Applications Be Isolated
Control [Access to Transaction Data]
Remote Censorship/ Deletion be Available
Protect Against Viruses/Malicious Code
Allow [Pirated Licensed/Copyrighted Content Upload/Download]
Prevent [Email Spam]
Allow [Peer-to-Peer Technology]
Retain [Control of Technology]
Send Unfiltered Spam
Hacker/ Malcious User
Intersect Transaction Data
Spread Viruses/ Malcious Code
Access Stored Data
Personal Information Be Gained
Control of Technology Be Obtained
Help
Hurt
Break
Make
Some +

UNIVERSITY of TORONTO

Thank you!

Questions?

References

- Anderson, R., “Trusted Computing' Frequently Asked Questions”, Retrieved July 2004 from www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- Falcone, R., Castelfranchi, C., “Social trust: A cognitive approach”, In C. Castelfranchi and Y.-H. Tan (ed.), *Trust and Deception in Virtual Societies*, Kluwer Academic Publishers, 2001, pp. 55-90.
- Gambetta, D. (ed.), *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, New York, 1988.
- Gans, G., Jarke, M., Kethers, S., Lakemeyer, G., “Continuous requirements management for organization networks: a (dis)trust-based approach”, *Requirements Engineering Journal, Special Issue RE'01*, Springer 8, 2003, pp. 4-22.
- Horkoff, J., *Using i* Models for Evaluation*, Masters Thesis, University of Toronto, Department of Computer Science, 2006.
- “Microsoft Next-Generation Secure Computing Base - Technical FAQ”, Retrieved July 2004 from www.microsoft.com/technet/Security/news/ngscb.mspx
- “OpenOME, an open-source requirements engineering tool”, Retrieved November 2005 from www.cs.toronto.edu/km/openome/
- *Trusted Computing Group Backgrounder*, Retrieved July 2004 from https://www.trustedcomputinggroup.org/
- Yu, E., “Modeling Organizations for Information Systems Requirements Engineering”, Proc. 1st IEEE International Symposium on Requirements Engineering, San Diego, California, USA, 1993, pp. 34-41.
- Yu, E., “Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering”, In *Proceedings of the 3rd IEEE Int. Symp. on Requirements Engineering (RE'97)*, 1997, Washington D.C., USA, pp. 226-235.