Economic Tussles in Federated Identity Management

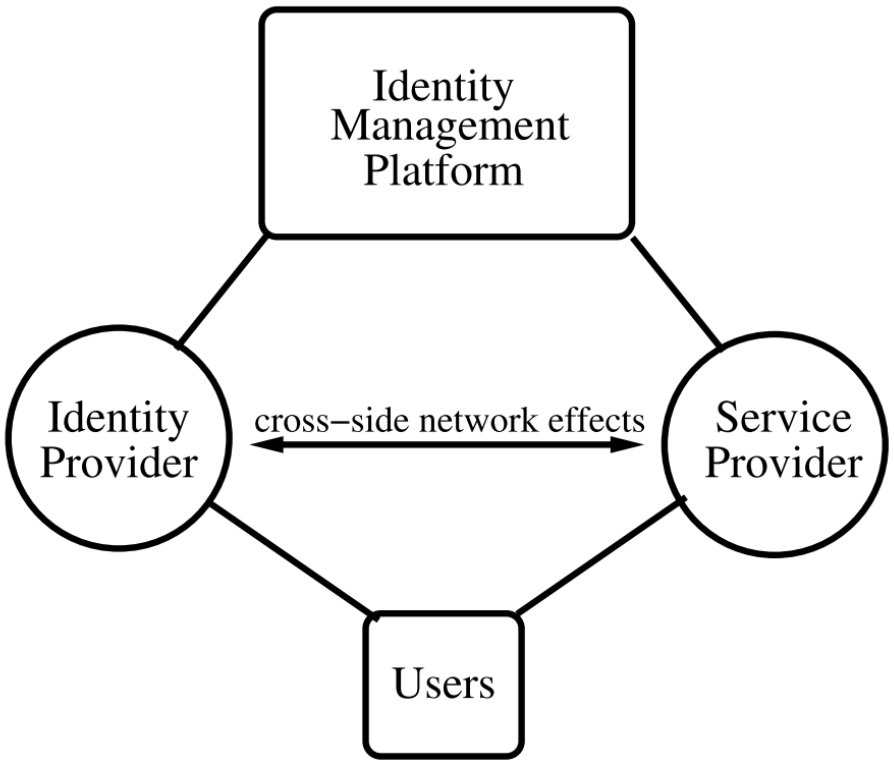
Tyler Moore
tylerm@smu.edu

joint work with
Susan Landau
susan.landau@privacyink.org

NIST/NSTIC IDTrust Workshop
March 14, 2012

HARVARD
School of Engineering and Applied Sciences

Federated Identity Management



- Two-sided market
  - Identity providers and service providers must attract users
  - Cross-side network effects
- Engineered system
  - Platform mediates the relationship between actors
  - Different levels of assurance of identity credentials
  - Rules for handling failures
  - Designed well, systems align interests of all stakeholders

FIM Use Cases

- Successful deployments
  - Shibboleth online sharing of library resources
  - InCommon/NIH research collaboration
  - Sun Microsystems outsourced services
  - Aetna's medical billing system
- Less successful deployments
  - Information sharing across law-enforcement agencies
  - OpenID standard for online authentication

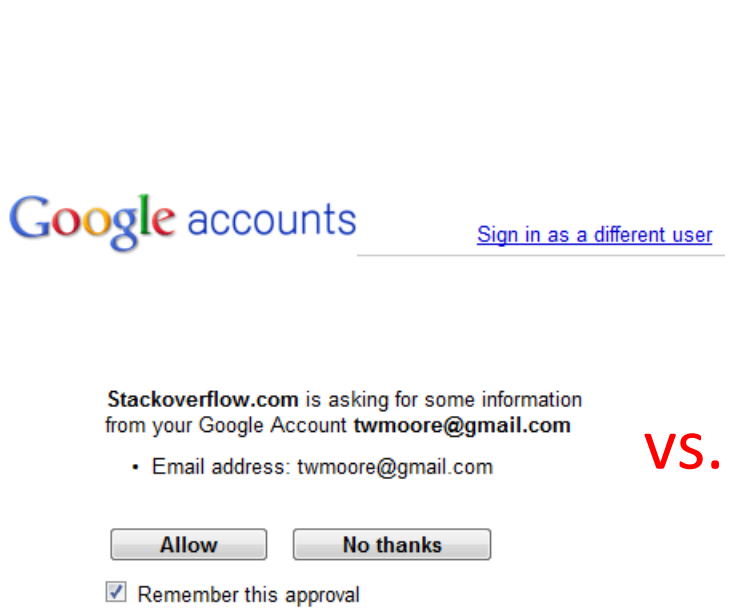
4 economic tussles that may arise when engineering a FIM system

1. Who gets to collect transactional data
2. Who sets the rules of authentication?
3. What happens when things go wrong?
4. Who gains and who loses from interoperability?

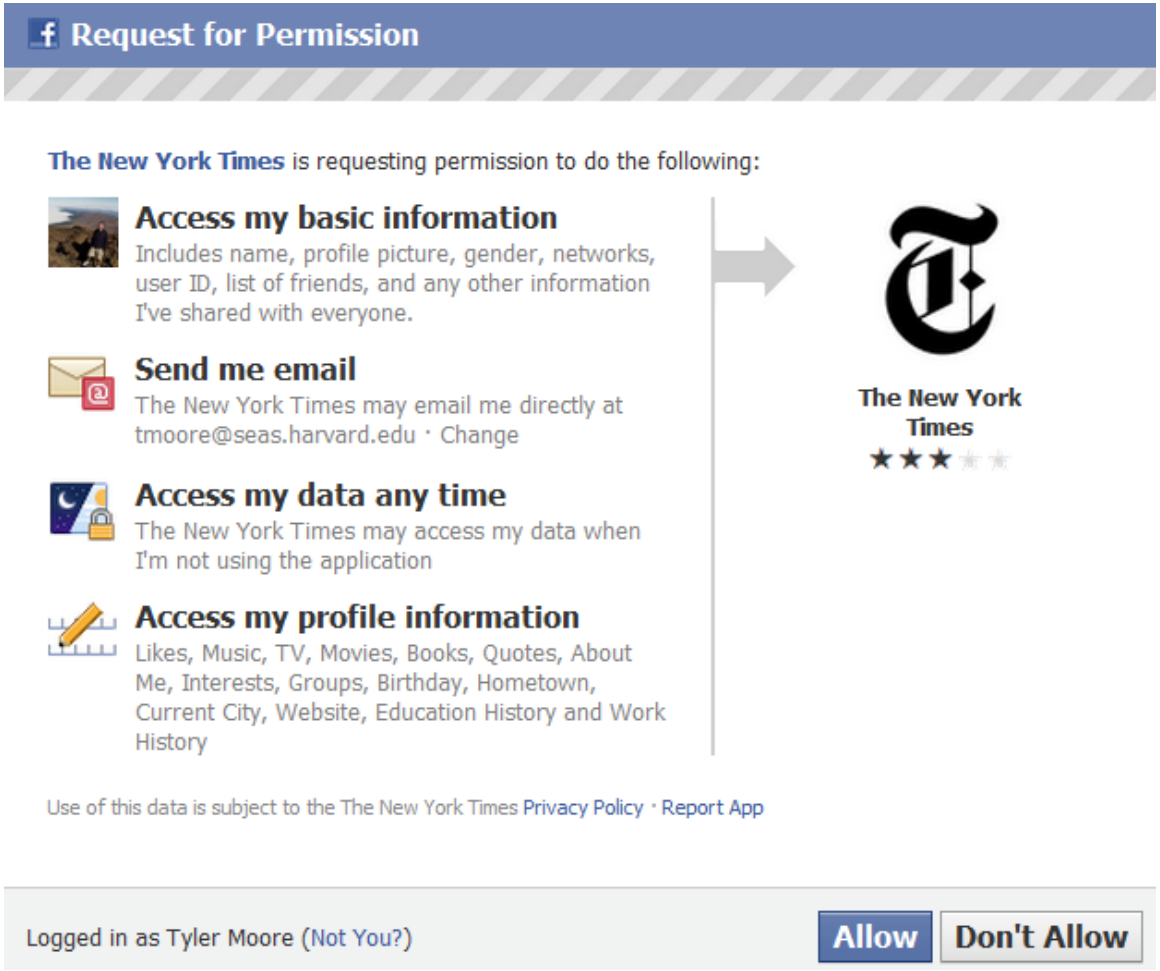
Tussle 1:
Who gets to collect transactional data?

- FIMs generate rich trail of user data as byproduct of transactions
- Which stakeholders (if any) are given access to transactional data can explain system's success
- In the web-authentication space, the transactional data is the key value
- If privacy-protection is a priority, then perhaps NSTIC should focus on other use cases

Facebook shares more extensive user data than OpenID can offer



vs.



Tussle 2: Who sets the rules of authentication?

- Identity management platforms offer huge first-mover advantage
  - Time to market matters more than robustness of authentication
  - Entrenched payment networks may be willing to tolerate higher levels of fraud
- Setting the right level of authentication is hard
  - Competitive IdPs want to attract users, and so want to make authentication easy (e.g., OpenID)
  - SPs may desire stronger authentication, and so ask for more stringent requirements that dampen uptake

Tussle 3: What happens when things go wrong?

- Two types of failure
  - IdP becomes unavailable, harming user-SP interaction
  - Unauthorized users incorrectly authenticated
- Clear allocation of responsibility for failure is key
  - Shibboleth: library serving as IdP clearly responsible
  - Payment cards: merchants and banks fight over who should pay for failure (e.g., PCI compliance rules)
- What's at stake also matters
  - *Low*: clarity less essential (web auth.)
  - *Large but easy to measure*: clarity essential (payments)
  - *Large and poorly understood:* clarity impossible?

Tussle 4: Who gains and who loses from interoperability?

- Key benefit to FIMs is that users authenticated by one IdP can be served by many SPs
- Yet the benefit (or risk) of improved interoperability may vary by stakeholder
- Global Federated Identity and Privilege Management (GFIPM) is designed to facilitate sharing among state and local law enforcement
  - Information sharing easy sell to IdPs – better access to intelligence
  - Yet sharing sensitive information with outsiders is a clear threat to SPs

Tussle Recap

	Tussle 1 Who Collects Trans. Data	Tussle 2 Who Sets Auth. Rules	Tussle 3 When Things Fail	Tussle 4 Interoperability Gains/Losses	Success?
Shibboleth	✓	✓	✓	✓	✓
NIH FIM	✓	✓	✓	✓	✓
Sun outsourcing	✓	✓	✓	✓	✓
Aetna's billing	✓	✓	✓	✓	✓
Clearances	✓	✓	✘	✘	✘
Open ID	✘	✘	✓	✘	✘
Payment networks	✓	✓	✓*	✓	✓

Insights & concluding remarks

- All stakeholders must gain from FIM to succeed
- Policy makers must ensure the interests of users are protected, especially wrt privacy
- Unresolved liability is but one way to fail
- Tackling the tussles simultaneously is essential
- For more: http://lyle.smu.edu/~tylerm/ http://privacyink.org/