Science and Technology:
Identity Theft: Policy Implications

K. A. Taipale
Executive Director, Center for Advanced Studies
Senior Fellow, World Policy Institute
Adjunct Professor of Law, NYLS

Presented at:
The Heritage Foundation
Washington, DC • November 2, 2005
Overview

• Privacy = Identity Theft

• Current remediation efforts are doomed to failure
  ▪ Data security is not a solution
  ▪ Breach notification is not a solution
  ▪ Federal preemption is a mistake and is not necessary

• A new model: Identity Registrar
  ▪ Eliminates Identity Theft
  ▪ Protects Privacy
Introduction

• What is identity?
  ▪ Who I say I am
  ▪ Who you say I am
  ▪ Who others say I am
• For our purposes:
  ▪ Identity is a set of claims for counterparty use
  ▪ Reputation is the authentication of those claims
• The “privacy” problem, who “owns” PII?
  ▪ Subject “owns” identity (rivalrous)
  ▪ Counterparties “owns” reputation (non-rivalrous)
Privacy (secrecy) = ID Theft

- Use of identifiers as authenticators
  - SSNs, DOBs, MMN, etc.
- System is based on wide-spread sharing of “semi-secrets”
  - But “secret” is a one-way street (info wants to be free)
  - Demise of practical obscurity - ubiquitous, persistent and proximate
- ID theft is claims/risk business process problem not a privacy problem (default=permit to default=deny, makes ID valuable)
- Thus, trying to enforce secrecy of PII increases ID theft
Remediation - Data Security

• There is need for data security
  ▪ Encryption for data
  ▪ Best practices for systems
  ▪ Liability vs. regulation

• But data security is not ID-theft solution
  ▪ Trying to enforce “secrecy” of “shared secrets”
  ▪ Secrecy is brittle and not recoverable
  ▪ Focus on data security exacerbates the problem
    • Creates greater “theft value”
    • False sense of security ~ complacency
Remediation - Notice

- Notice as choice
  - Prior to disclosure - notice is actionable (FIPs)
  - After breach - ??? (externality problem)

- Practical problems/effects
  - What trigger (define and decide)
  - What risk (data breach/stolen laptop ~ ID theft)
  - Notice overload
  - Proven ineffective
Remediation - preemption

• Preemption = lock in
  ▪ Of existing business models
  ▪ Of existing market participants
  ▪ LCD vs best practices
  ▪ Precludes innovation and experimentation
  ▪ Undermines Federalism

• Preemption is unnecessary
  ▪ Based on outmoded mfg./product compliance model
  ▪ Technical solution - rules-based processing - is not only possible ... but needed through-out IS (jump-start market)
Identity Registrar
eliminates identity theft and protects privacy

• Identity Registrar
  ▪ Voluntary system, accommodates all existing business models
  ▪ Create an authoritative site/system (DNS) (FTC, ICAAN, ?)
  ▪ Make your name, SSN, and certain protected contact information publicly available
    • Designate your claims - point to Identity Broker
    • Subject gains authoritative control over identity
  ▪ Service providers (credit issuers, etc.) who use the system retain their current exemption from legal liability for misidentification
    • Additional source not exclusive source (more information is good)
    • Counterparty retains control over reputation assessment
  ▪ Service providers who did not use the system would be liable for misidentification (defamation, invasion of privacy, negligence)
Identity registrar (cont.)

- Identity Broker would be authorized repository for authentication and could offer varying levels of service
  - Verification services
- Multiple identities for specific purposes. Brokers could be employers, unions, banks, data aggregators, etc.
- Controlled contact (cut-out, filter) (verified counterparty, call back, etc.)
- Subject (~ind) designated verification (and disclosure) process
  - Fraud alert, file freeze, opt out/opt in, extensible/scalable/auto
- Minimal required legislation
Conclusions

The solution to ID Theft is business process change

What is needed is a technologically-enabled information society paradigm to replace the paper-dependant manufacturing model in use