

# PRIVACY and CYBERSECURITY

Tom Oscherwitz

Vice President of Government Affairs and Chief Privacy Officer

ID Analytics, Inc.

1:15pm

Washington D.C.

February 14<sup>th</sup>, 2010

---



# The Nexus of Identity, Privacy, and Cybersecurity

The Connection is Not New

- **CSIS Report – Securing Cyberspace for the 44<sup>th</sup> Presidency**

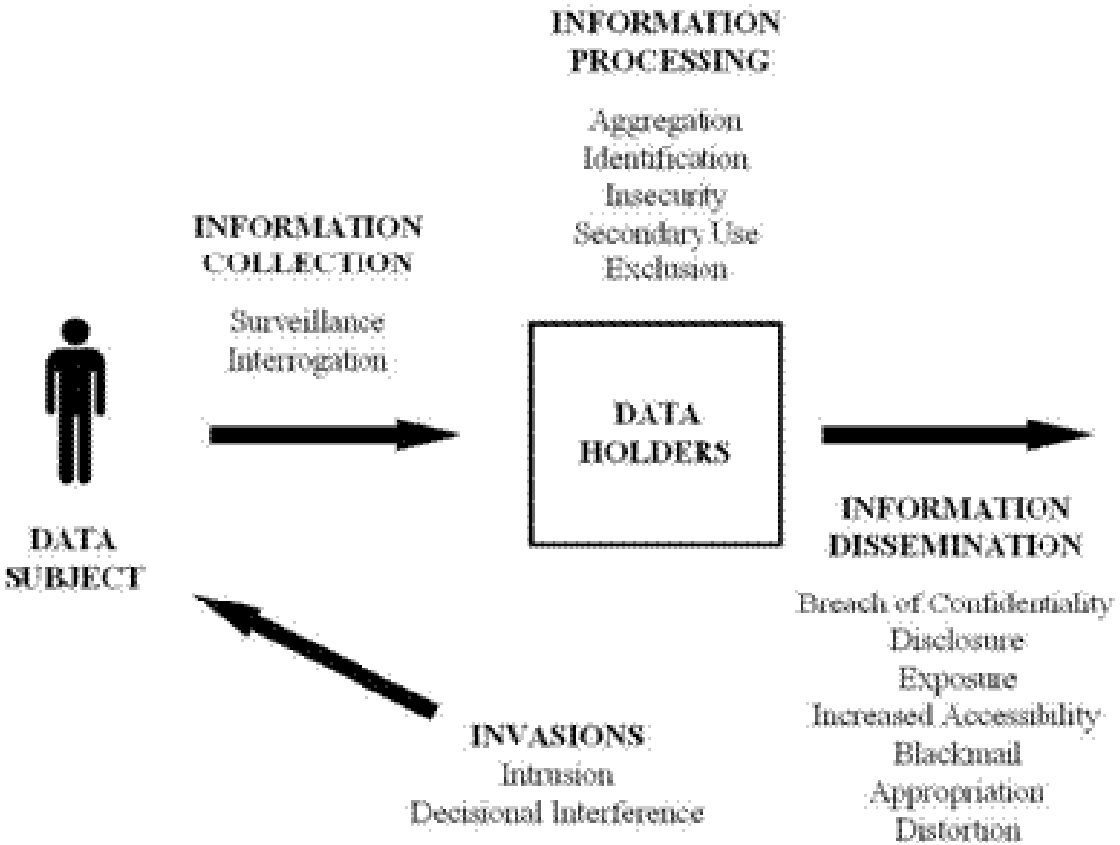
“The United States should make strong authentication, of identity, based on robust in-person proofing and through verification of devices, a mandatory requirement for critical cyber infrastructures.”

- **President’s 60 Day Cybersecurity Review**

- Identity management part of Near Term Action Plan:
- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation

- **NSTAC Identity Issues Task Force**

# Professor Daniel Solove's Taxonomy of Privacy



Cybersecurity implicates identification and other privacy problems

# How are Identities Managed Today?

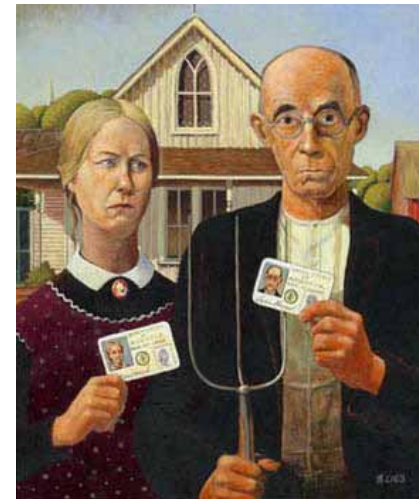
- **What you know**

- Username, password, security phrase
- Q/A sessions: mother's maiden name, favorite pet, best friend's name



- **What you have**

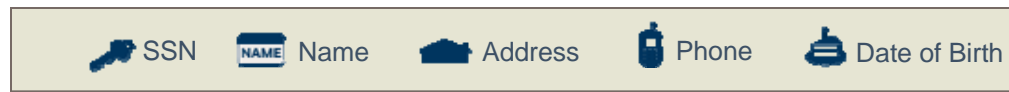
- Photo id, secure token, smartcard
- Biometrics: fingerprint, hand geometry, iris scan



# How Identities are Managed Today

- **How you behave**

- Remotely observed behavior: transactions, online motion (clicks, typing)
- Relationship connectivity: identity graphs



- **FFIEC Guidance** on “Authentication in **an Internet** Banking Environment” gives a good (though dated) general description of multi-factor technologies
  - (See [http://www.ffiec.gov/pdf/authentication\\_guidance.pdf](http://www.ffiec.gov/pdf/authentication_guidance.pdf))

---



## Bringing People into the System

- **Verification technologies have privacy implications**

- Privacy implications for individual being verified

- What data is being collected?
- How long is collected data being stored?
- Subject to further or unrelated use?
- User Control over information being shared?

- Privacy implications of poor verification

- Errors in records (e.g. mixing up health records)
- Identity fraud
- Exposure of private information (e.g. 3<sup>rd</sup> party accessing personal email)
- Cyberthreats/Granting the wrong person access to a system

---



# PRIVACY ISSUES ACROSS IAM LIFECYCLE

- **While users in Systems**
- Collection/Use Purposes
  - Why is the data required and how is it actually being used?
  - What governance exists over use of data?
  - What disclosures are being made?
  - Used for unrelated purposes (mission creep)
- **Governance and Process over Departures**
  - Failure to separate employee from system



## Best Practices

- **There is no single correct answer for IAM of employees or customers.**
  - Needs to be based on size & complexity of organization
  - Take a Risk-Based Approach
- **Pursue multi-layered authentication models capable of being tailored to evolving risk**
- **OECD privacy principles can inform decision-making (e.g. purpose limitation, keep only what you need)**

# Questions

Tom Oscherwitz

Vice President of Government Affairs and Chief Privacy Officer

ID Analytics, Inc.

[toscherwitz@idanalytics.com](mailto:toscherwitz@idanalytics.com)