Veterans Administration Breach

- 26.5 million veterans’ information stolen
- Employee did not follow basic VA security policy
- Thieves did not seem to be seeking identity information
- Why is this, what would formerly was thought of as a low-risk theft, of such concern?
“...a 23-year-old methamphetamine user showed officers a new way to steal identities.”

“...he pulled up a local divorce document listing the parties' names, addresses and bank account numbers, along with scans of their signatures.... all he needed to print checks in his victims' names”

“Police officers and prosecutors in Phoenix knew of just two cases involving public records, but most victims do not know how their identities are stolen.”
Federal privacy rules have fallen behind

“The government cannot adequately assure the public that all legislated individual privacy rights are being protected.”

Lack of Leadership

- Failure to address aging Privacy Act
- Full Privacy Act guidance not overhauled since 1975
- OMB Chief Privacy Counselor position not renewed
- No best practices for privacy impact assessments (PIAs)
- Lack of guidance on protecting privacy in agency use of commercial data
- Mixed messages in OMB memos to agencies
Commercial Data in Government

- Guidance needed to clarify when Privacy Act applies to commercial data
  - Private Collection Under Government Contract
  - Receipt of Commercial Data
  - Merging of Commercial and Government Data
  - Direct Use of Commercial Data (on private server)

- PIAs should be required for any use

- Agencies must look beyond letter of current law to protect data
Privacy Act Issues

- “Systems of Records” — describes a ‘70s style flat database and not relational or distributed databases
- “Routine Use” Exemption — overused and underdefined
- Commercial Data — Section(m) has always been unclear and
Contact

Ari Schwartz
Deputy Director
Center for Democracy & Technology
202-637-9800
ari@cdt.org
http://www.cdt.org