# National Geospatial Advisory Committee

**Robert Gellman**
Privacy Consultant
Washington DC

www.bobgellman.com
bob@bobgellman.com

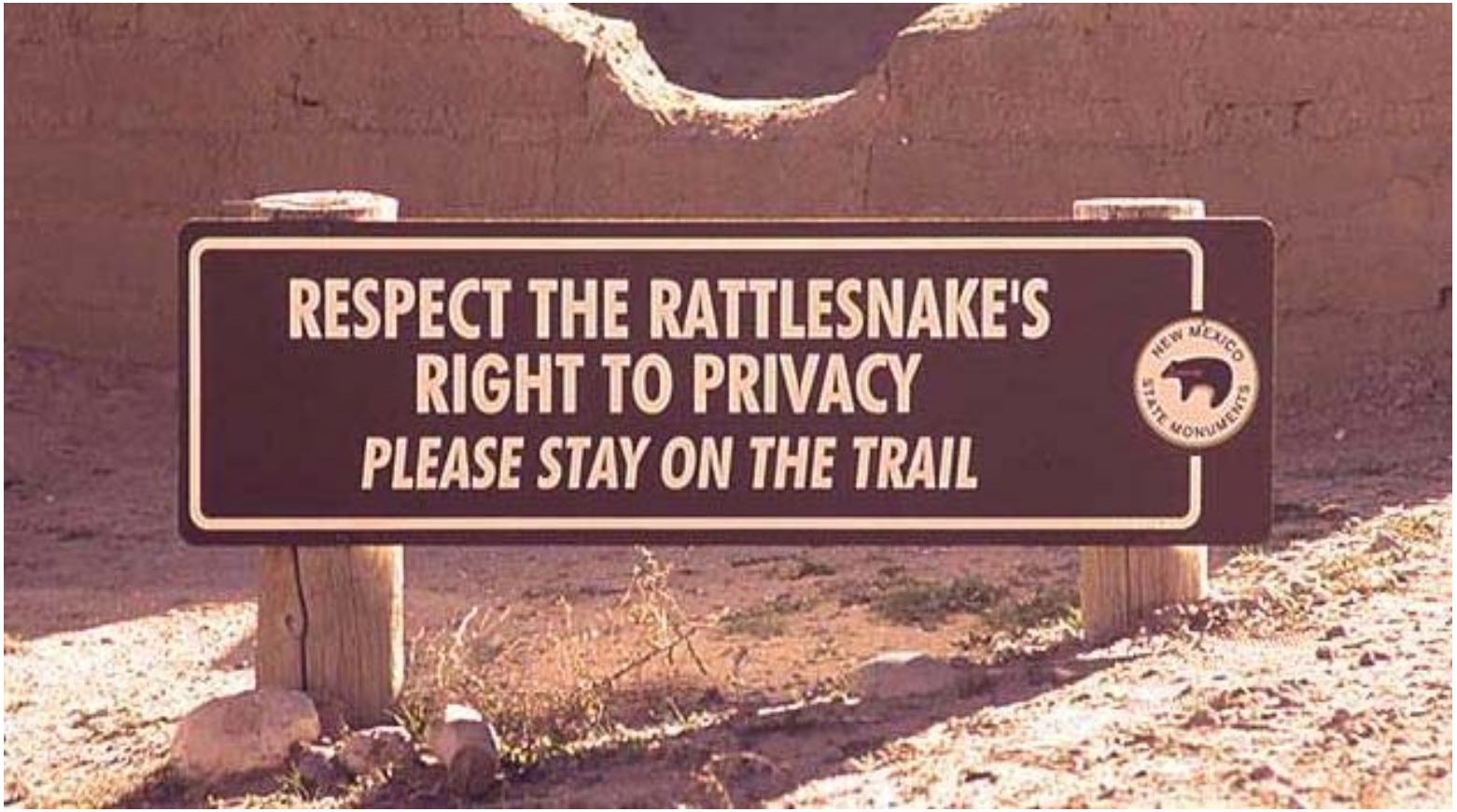
9/18/12

# What is Privacy I

Abortion/Contraception
Keep Government out of House/Papers
Free Speech
Education of Children
Right to Assemble
Right to Vote (secret ballot)

Self-incrimination
Personal Information
Practice Religion
Private Conversations
Freedom from Surveillance
Join a Party/Union
et cetera

# What is Privacy II



# What is Privacy III

- **Privacy**: Interests of (Living?) Individuals
- **Confidentiality**: Interest of Individuals and Legal Persons (corporations)
- **Security**: Technical and administrative measures to protect data against loss or unauthorized disclosure, access, destruction, alteration, or use

# What is Privacy IV

*Data Protection*: Rules about the collection, maintenance, disclosure, and use of personal information

Also: Records Privacy; Information Privacy

# Fair Information Practices

Collection Limitation
Data Quality
Purpose Specification
Use Limitation
Security Safeguards
Openness
Individual Participation
Accountability

History at http://bobgellman.com/rg-docs/rg-FIPshistory.pdf

# Fair Information Practices 1 & 2

1) **Principle of Openness**, which provides that the existence of record-keeping systems and databanks containing data about individuals be publicly known, along with a description of main purpose and uses of the data. (Also called Transparency).

2) **Principle of Individual Participation**, which provides that each individual should have a right to see any data about himself or herself and to correct or remove any data that is not timely, accurate relevant, or complete.

# Fair Information Practices 3 & 4

3) **Principle of Collection Limitation**, which provides that there should be limits to the collection of personal data, that data should be collected by lawful and fair means, and that data should be collected, where appropriate, with the knowledge or consent of the subject.

**4) Principle of Data Quality**, which provides that personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete, and timely.

# Fair Information Practices 5 & 6

5) **Principle of Use Limitation**, which provides that there must be limits to the internal uses of personal data and that the data should be used only for the purposes specified at the time of collection.

6) **Principle of Disclosure Limitation**, which provides that personal data should not be communicated externally without the consent of the data subject or other legal authority.

# Fair Information Practices 7 & 8

7) **The Principle of Security**, which provides that personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.

8) **The Principle of Accountability**, which provides that record keepers should be accountable for complying with fair information practices.

# Expectation of Privacy

A a **reasonable expectation of privacy** exists if (1) a person has exhibited an actual (subjective) expectation of privacy; and (2) that expectation is one that society is prepared to recognize as reasonable.

*Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)

# Standards of Identifiability

- HIPAA. 18 elements. Expert. 45 CFR 164.514 (health records)
- Privacy Act of 1974: name, or the identifying number, symbol, or other identifying particular assigned to the individual. 5 USC § 552a(4)) (definition of record)
- CIPSEA: identifiable form means "any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means." 44 U.S.C. § 3501 note §502(4).
- EU Data Protection Working Party paper on the meaning of *personal data* at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf164.514