PRIVACY ASSOCIATES INTERNATIONAL LLC

Privacy Past and Future

ISSA

January 21, 2016

Keith A. Cheresko
Principal, Privacy Associates International LLC

© 2016 all rights reserved

Purpose

- What is Privacy?
- American Privacy Past - How we got to here
- Some International Privacy – OECD, EU

What is Privacy?

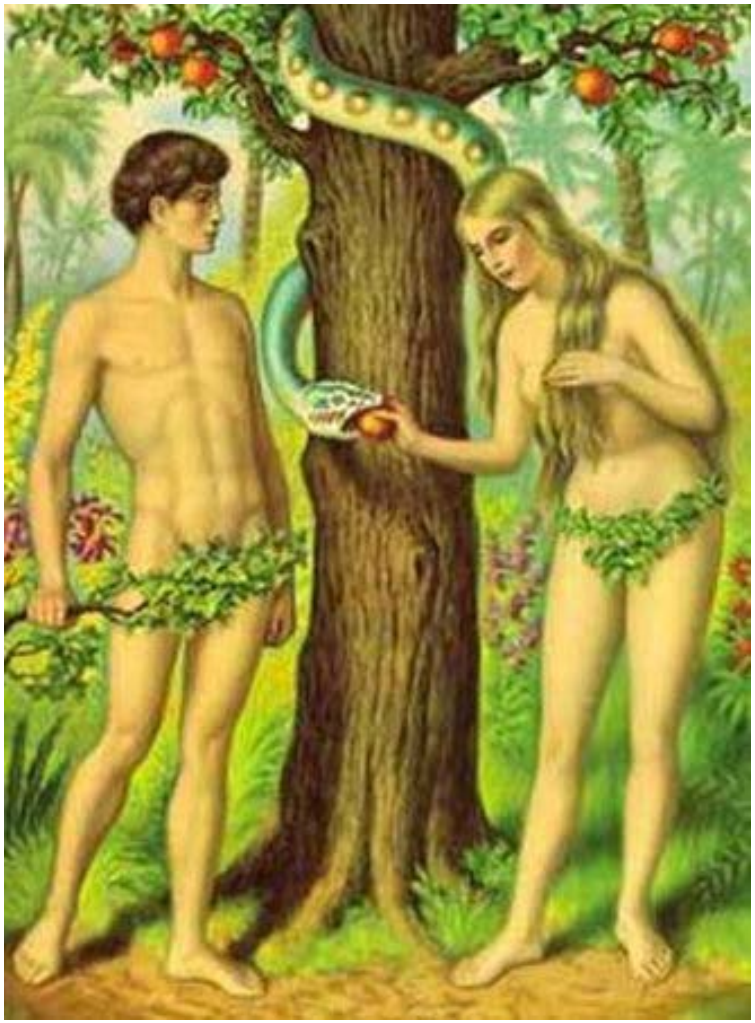
- Different meanings to different people
- Large element cultural
- Hundreds of definitions, but most involve the ability of a person to control information about himself, or access to himself

Where Did Privacy Come From?

Privacy concerns have existed for long time

The Epic of Gilgamesh

Adam & Eve



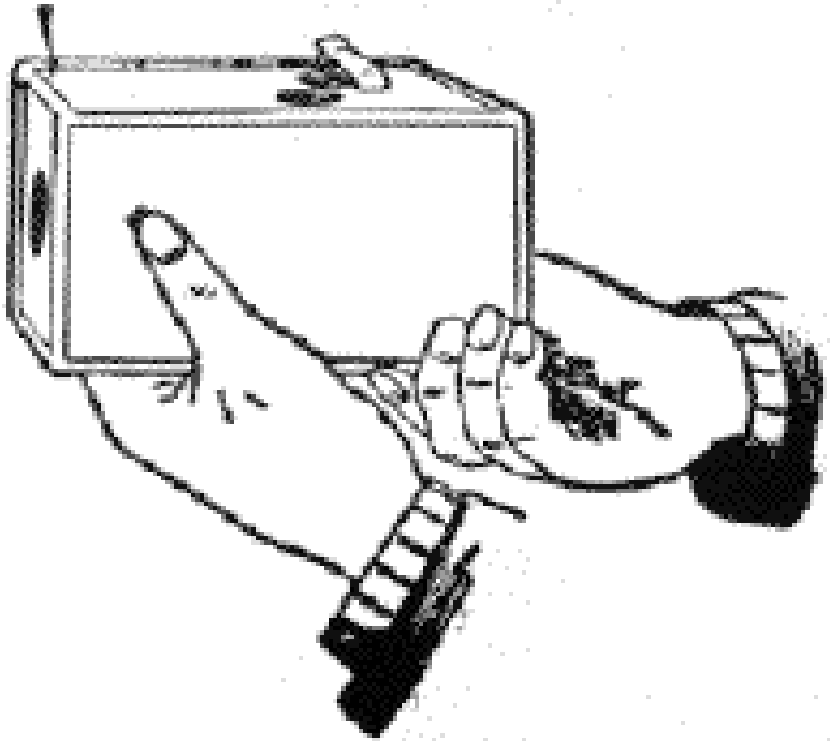
Code of Hammurabi

Justices of the Peace Act, England 1361

American Privacy

Has its roots in dazzling new technology

THE KODAK CAMERA



100 Instantaneous Pictures!

Anybody can use it.

No knowledge of photography is necessary.

The latest and best outfit for amateurs.

Send for descriptive circulars.

Price $25.00.

The Eastman Dry Plate & Film Co.

ROCHESTER, N. Y.

American Right to Privacy

- The Warren & Brandeis Article: The Right to Privacy (1890)

  - One of the most famous and influential law journal article in US legal history

  - Source of the idea that a right to privacy exists in American law

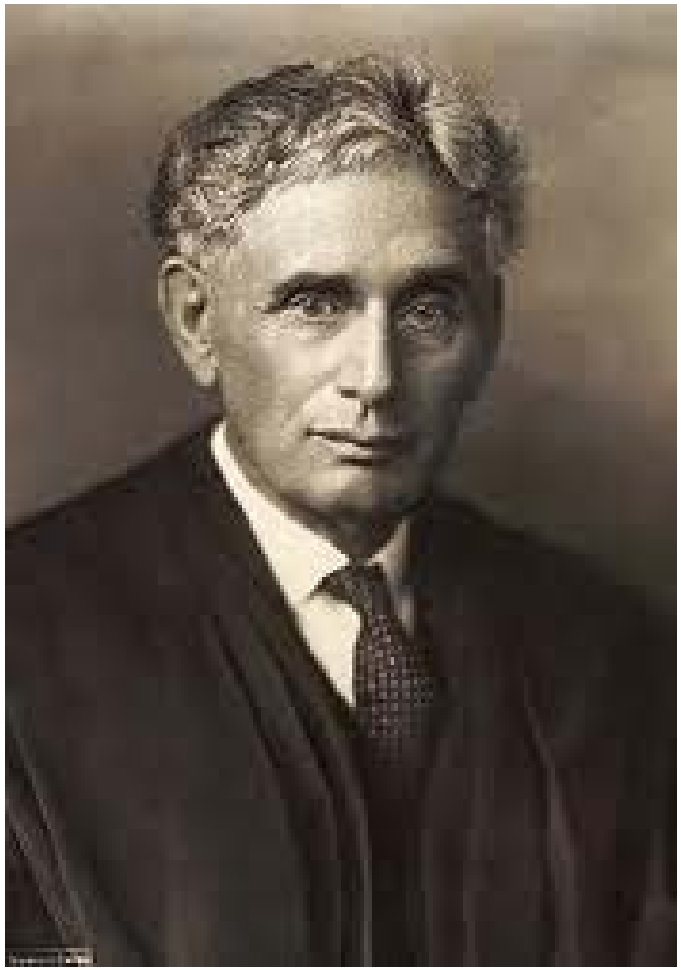
- Written as reaction to the "yellow press"

  - Gossip and hearsay articles

  - Publicized private facts

  - Threatening new technology "instantaneous photography" exacerbated problem

“The right to be left alone”



American Invasion of Privacy

- The article eventually led to the recognition in American law of the concept of Invasion of Privacy
- Invasion of Privacy is a name given to a collection of actions for which people can bring lawsuits:
  - Intrusion upon seclusion
  - Public disclosure of private facts
  - False light
  - Appropriation of name or likeness

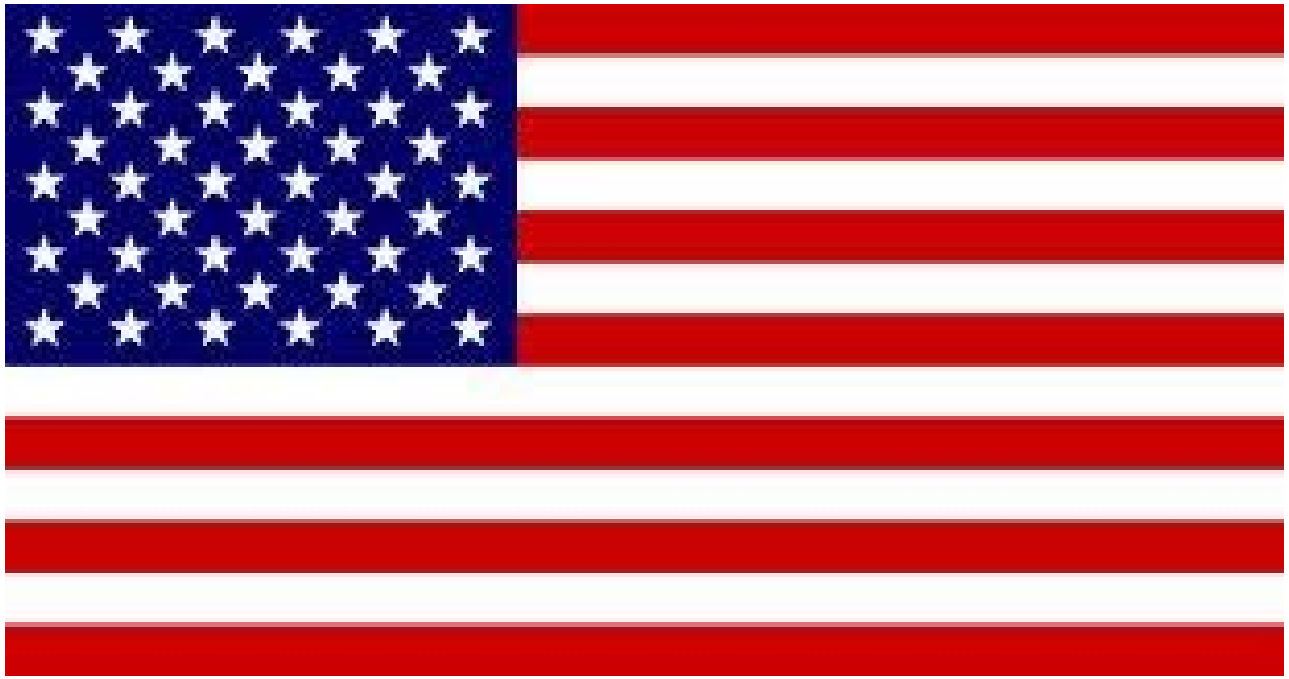
I remember something about the Gilgamesh from 8th grade World History class, but what does all this have to do with me?

Information Privacy

- A category of privacy rights
- Importance has been magnified by the Information Technology revolution and economic globalization
- Relates to the interest a person has in controlling his or her personal information
- Relevant to all organizations that handle personal information
- Applicable rules differ, but some basic concepts are the same

PAI

US Approach to Information Privacy



US Statutory Approach to Privacy

- US now a hodge-podge of hundreds of federal and state privacy laws that deal with privacy in different contexts
- Each statue is aimed at different problem and has different definitions of what constitutes personal information
- Incomprehensible system for those outside the US (and many of us inside the US)

Examples of Federal Laws

- **Cable Communications Policy Act**
- **CAN-SPAM Act**
- **Children's Online Privacy Protection Act**
- **Computer Matching and Privacy Protection Act**
- **Consumer Credit Reporting Reform Act**
- **Driver's Privacy Protection Act**
- **Electronic Communications Privacy Act (ECPA)**
- **Electronic Funds Transfer Act**
- **Electronic Signatures in Global and National Commerce Act**
- **Employee Polygraph Protection Act**
- **Fair and Accurate Credit Transaction Act (FACTA)**
- **Fair Credit Reporting Act (FCRA)**
- **Family Educational Rights and Privacy Act**
- **Financial Services Modernization Act (aka Gramm-Leach-Bliley)**
- **Foreign Intelligence Surveillance Act**
- **Freedom of Information Act**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Identity Theft and Assumption Deterrence Act**
- **Privacy Act of 1974**
- **Privacy Protection Act of 1980**
- **Right to Financial Privacy Act**
- **Telecommunications Act**
- **Telemarketing and Consumer Fraud Act**
- **Video Privacy Protection Act**
- **Video Voyeurism Prevention Act**

Selected Areas of State Legislation

- Identity theft protection
- Security breach notification
- Social security number protection
- Marketing
- Spyware and adware
- Radio frequency identification devices
- Insurance
- Vehicle data event recorders
- Background checks

International Privacy

Organisation for Economic Co-operation and Development (OECD)

- An influential international economic organization of 34 countries founded in 1961 to stimulate economic progress and world trade
- In 1977 developed privacy guidelines that have become the touchstone of modern privacy law in the international context
- Not laws, but have become the fundamental basis of information privacy laws

PAI

The Eight OECD Guidelines

1. **Collection Limitation Principle:**

   "There should be limits to the collection of personal data and any such data should be collected by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject."

2. **Data Quality Principle:**

   "Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."

PAI

OECD Guidelines

3. **Purpose Specification Principle:**

   "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

OECD Guidelines

4. Use Limitation Principle

"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law. "

5. Security Safeguards Principle:

"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."

OECD Guidelines

6. Openness Principle:

"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."

OECD Guidelines

7. Individual Participation Principle:

"An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."

PAI

OECD Guidelines

8. Accountibility Principle:

"A data controller should be accountable for complying with measures which give effect to the principles stated above."

…

Guidelines supplemented in 1980 with Statement on International Data Flows

European Union Approach to Information Privacy

European Cultural Attitude Toward Personal Information Differs From US

- Personal information collection is viewed as something to be avoided unless absolutely necessary
- Thus, European countries regulate the ***collection and transmission*** of personal information, as opposed to US regulation of ***misuse*** of personal information
- Human rights issue in Europe as opposed to annoyance/identity theft issue
- WWII experience

EU Approach to Information Privacy Most Influential Globally

- Embodied in the 1995 Directive on Data Protection
- Data Protection Directive sets minimum standards for privacy laws in all 27 EU member states
- Also followed in non-EU European countries: Iceland, Liechtenstein, Norway and Switzerland
- Transitioning to new a new General Data Protection Regulation the "GDPR"

EU Approach

- Forms the general model for many laws outside of Europe, eg: Argentina, Australia (for consumer info), Canada, Peru, Israel, New Zealand, Russia
- Establishes a bureaucracy in each country to administer that country's version of the law
- Must register the maintenance of databases with the bureaucracy and ask permission/notify them of certain actions

EU Approach

- “Personal data” broadly defined: includes any information relating to an identified or identifiable natural person
- “Sensitive Personal Data” enjoys stricter protections
- Cannot “process” personal data without a legal basis
- “Process” includes: collect, record, organize, store, use, alter, etc.

Legal Bases for Domestic "Processing" of Personal Information Under EU Directive

- Unambiguous consent
- Necessary for performance of contract to which data subject is party
- Necessary for compliance with legal obligation to which controller is subject
- Necessary to protect vital interests of data subject
- Necessary for performance of tasks carried in public interest or exercise of official authority
- Necessary for purposes of the legitimate interests pursued by controller or by the third party/ies to whom data are disclosed, except where such interests are overridden by the interest for fundamental rights and freedoms on the data subject that require protection

PAI

Must Further Comply with Details of National Law Related to Basic Principles when Processing Data

- Personal data must be fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Personal data must be accurate
- Not kept longer than necessary
- Must be processed in accordance with the data subject's rights (e.g. right to be informed and right of access)
- Personal data are to be kept secure
- Personal data may not be transferred to countries without adequate protection

My Head Hurts

Contact Information

Keith Cheresko, Principal

Privacy Associates International LLC

40777 Lenox Park Drive, Suite 100

Novi, Michigan 48377

248.535.2819

kcheresko@privassoc.com

www.privassoc.com