The end of Privacy ??

Murat Kantarcioglu

Privacy Under Attack

- In 1996, %24 of Americans has “personally experienced a privacy invasion” (%19 in 1978)
- Privacy vs. Convenience Trade off ??
  - In 1960s, some said that polluting the environment is required for development
- Right to privacy
- “Right to be let alone”

What Do We Mean By Privacy?

- Privacy is not just about hiding things
- Privacy is related to self-possession, autonomy, and integrity
- Privacy is about the woman who is afraid of to use the Internet to organize her community against a proposed toxic dump…….

Right to Privacy?

- "The right to be left alone"
- Explicit right to privacy is given in constitutions, laws and international treaties
- People want to have privacy:
  - Objections to Intel's chip sets unique identification number
  - Objections to National Database of Driver License Images

Role of Government

- Privacy is not a priority of the Government
- Regulations are needed for privacy.
  - Fair Credit Reporting Act
- Code of Fair Information Practices:
  - No secret personal data storage
  - Individual's right to know what is stored
  - No unintended use without consent
  - Right to correct or amend stored data
  - Reliable and Correct Data Storage

Public Concerns Over Privacy

- Lotus Development Corp and Equifax's "Lotus marketplace: Households"
  - **Project Canceled**
- Lexis-Nexis display of SSN
  - Due to protests, it took 11 days to change
- SSA's tax information publishing
  - **Service Shut Down**

Law of Unintended Consequences

- SSN was developed related to social security act
- SSN is even used for identifying students
- Cell phones are used for payments
- Lasers are used in DVD players
- What will be the DNA used for???

Identity Theft

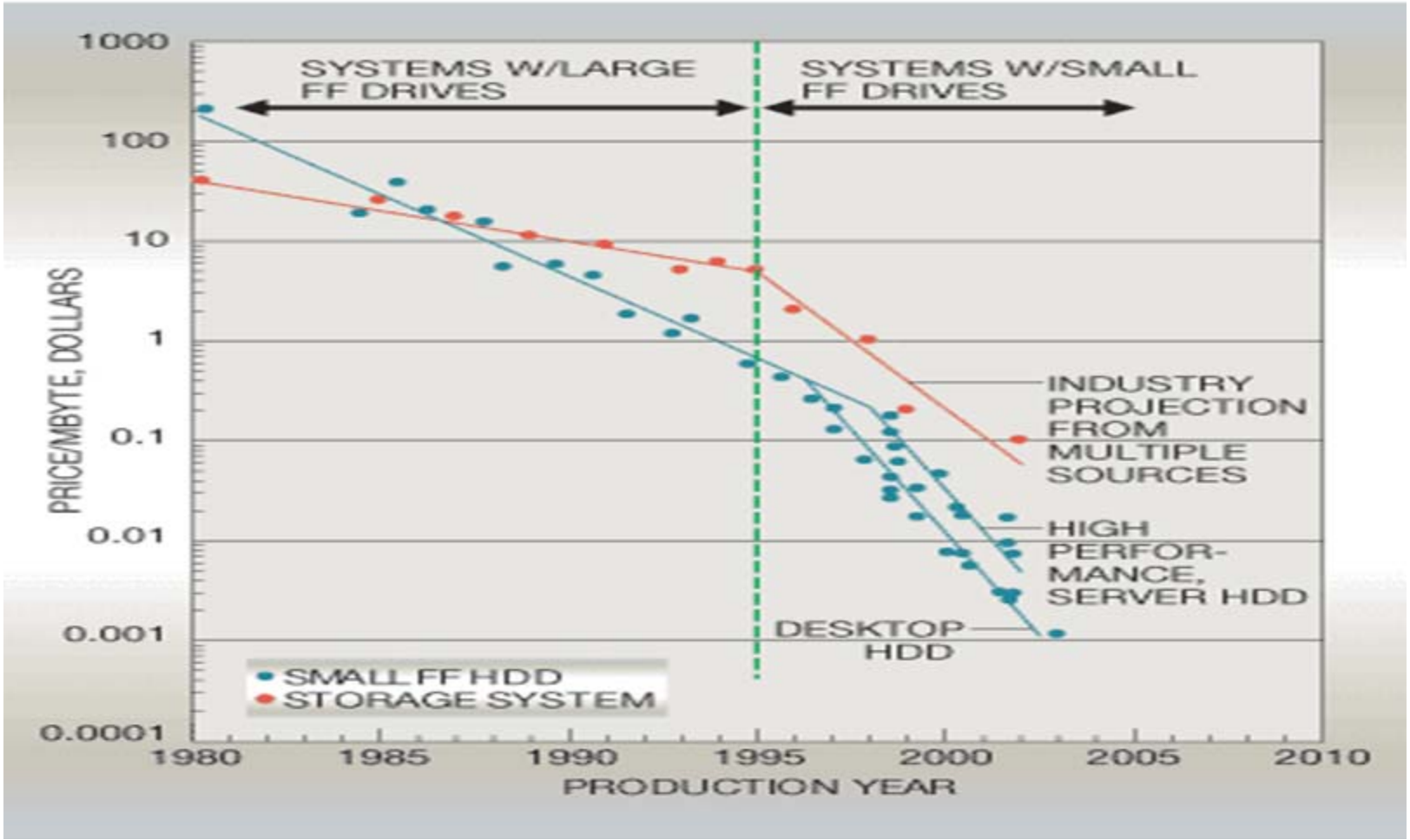
- Huge increase in identity thefts
- On average, it takes four years to clear your name
- No right to sue for personal suffering
- Market solutions do not work
  - No incentive for financial companies
- Simple solutions may help
  - **NO INCENTIVE FOR COMPANIES!!!!**

Abundance of Data

- Increasing storage of personal data
  - Credit card records
  - Phone records
  - Health care data
  - E-mails
  - BMV Records
  - Surveillance Cameras

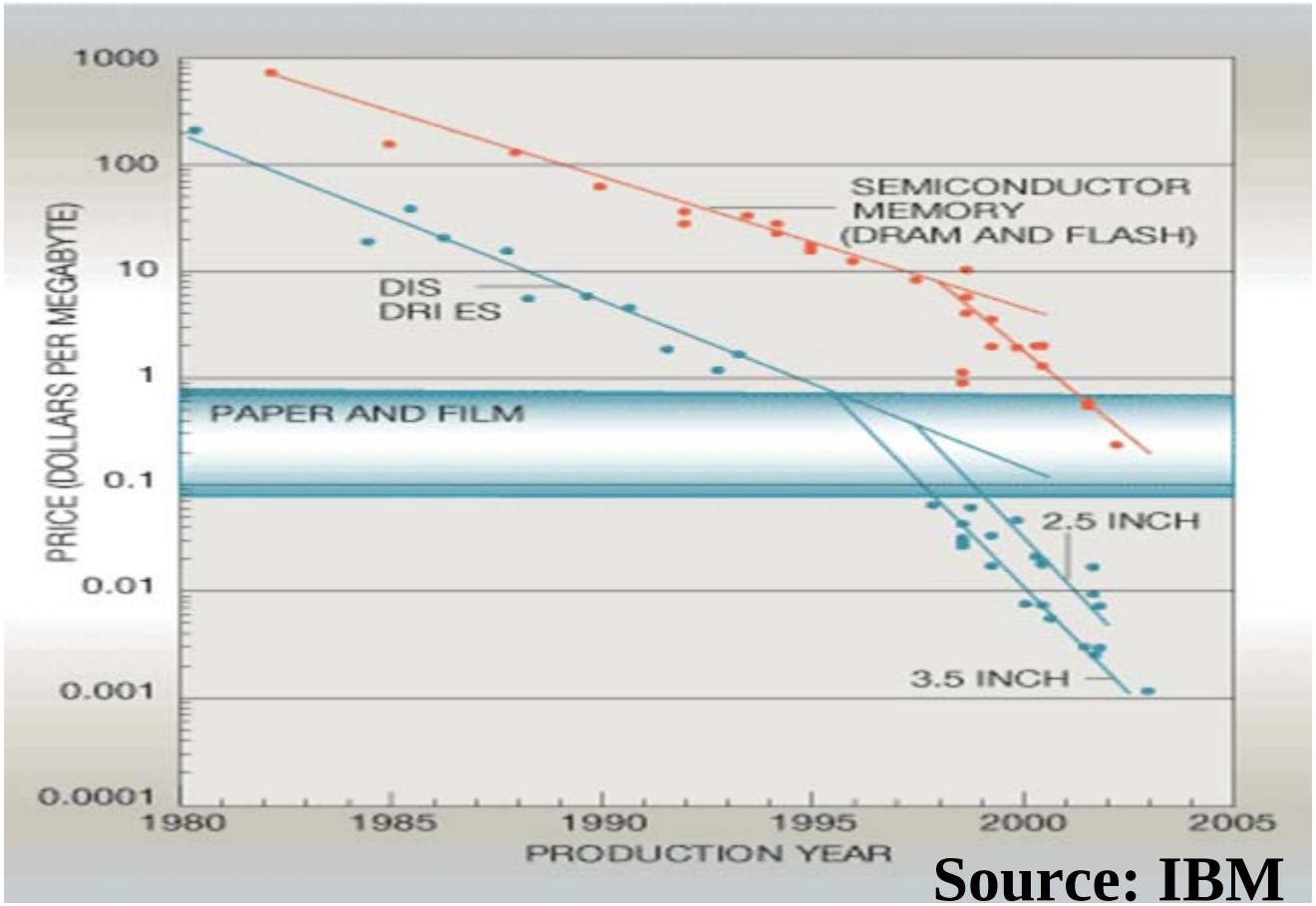
Decreasing Storage Costs

Figure 6 Cost of storage at the disk drive and system level



Decreasing Storage Costs

Figure 7 Cost of storage for disk drive, paper, film, and semiconductor memory



Source: IBM

Decreasing Computation Costs

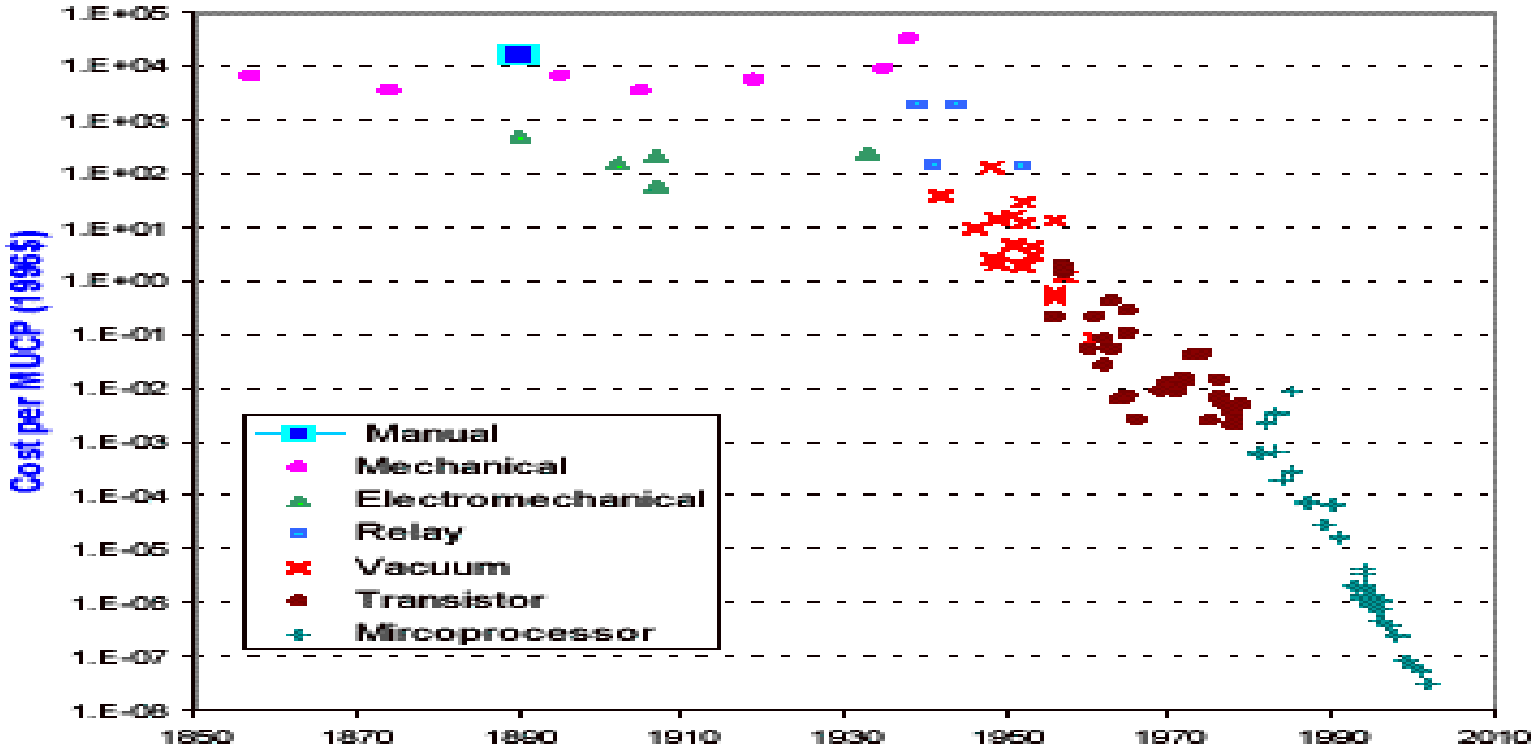


Figure 2. The cost of computer power for different technologies

Source: William Nordhaus

Convenience vs Privacy

- Legitimate Usage of Tracking technologies
  - Safer Streets
  - Cheaper Communications
  - Better government services
  - Easy and personalized shopping
- Hard to measure the value of privacy

New Threats to Privacy

- DNA Databases for medical research
  - Identifying individuals vs. Cheap Drugs
- Cheap tiny microphones
- Small video cameras
- Intelligent software
- Biometrics
- RFID chips
- Intelligent Homes/Clothes…..

Possible Solutions

- More laws…
  - Right to sue for privacy violation! (not yet)
  - EU Data Protection directive
    - Requires explicit consent for processing
    - Restricts the usage of the data for intended purpose
  - California Database Breach Notification Act
  - HIPAA (more on this later)
- Problems with enforcement
- No right to sue for damages

Possible solutions

- Marked based approach:
  - Not enough interest from customers yet.
  - FTC survey found only %2 of 1400 sites has privacy policies
  - Enforcement issues
- Not enough demand for privacy technologies
  - www.anonymizer.com
  - Digital cash

Possible Solutions

- Information mediators
- Transparent Society
- Technology
  - Technological solutions will be our focus.

HIPAA

- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
  - Public Law 104-191 (August 21, 1996)

HIPAA's Privacy Regulations

- HIPAA required that the Secretary of Health and Human Services ("HHS") to issue privacy regulations if, and only if, Congress did not enact privacy legislation within three years of the passage of HIPAA.
  - Congress did not enact legislation

HHS' Privacy Rule

- Three years and three months after the passage of HIPAA, HHS developed a proposed Privacy Rule and released it for public comment.
  - 52,000 public comments
  - Finalized on December 28, 2000.

HHS' Privacy Rule Revisions

- March 2002 Revision Proposal:
  - 11,000 public comments
  - Adopted on August 14, 2002

Summary of the Privacy Rule

- HIPAA legislation passed by Congress contained a series of sections now known as the “Administrative Simplification provisions”
  - Under this provision, HHS is required to publish documents such at the “Summary of the Privacy Rule” which we read.

Inclusion in the Privacy Rule

Health Plans	Health Care Providers	Health Care Clearinghouses
Unless: **- Group plan of less than 50 people ran by the employer** **- Government funded programs that are "not health plans"**	**Unless:** **- Provider does not have a "standard" means of transaction of health care information** **(ex: e-mail)**	**Unless:** **- Clearinghouse is action only as a business associate which doesn't receive personally identifiable information**

Scope of the Privacy Rule

- Privacy rule protects all
  - “individually identifiable health information”
  - held or transmitted
  - by a covered entity or business associates

- Information called “protected health information” (PHI)

Scope of PHI

- An individuals past, present, or future:
  - Physical heath condition
  - Mental health condition
  - Payment of health care

- An individual health care provision.

…which there is a “reasonable basis to believe” the information is personally identifiable

… which isn’t an employee record held by the company of employment

Principle of Disclosure

- The Privacy Rule establishes a list of acceptable and unacceptable ways to use PHI.
  - Privacy Rule attempts to be a ‘catch-all’ law for privacy
- The Privacy Rule may be waived by a signature of a patient.
  - Q: How many things do you sign when you go to the doctor?
  - Q: Do you know what they say?
  - Q: Do you really have a choice to not sign then?

Principle of Disclosure

- The Privacy Rule does, however, ensure that individuals have access to the information stored about them.
  - Also allows HHS to view your medical records when they're "undertaking a compliance investigation"

De-identified Health Information

- No restrictions on the use or disclosure of de-identified health information
- A de-identification is achieved
  - by a formal determination by a qualified statistician or
  - Removal of certain identifiers (i.e., safe harbor rule.)

Explicitly Acceptable Disclosures

- Disclosure to the individual (required)
- Disclosure to: (allowed without consent)
  - Treatment Operations
  - Payment Operations
  - Health Care Operations

Explicitly Acceptable Disclosures

- Disclosures with “Opportunity to Object”
  - Ex: Directory of patients
  - Ex: Notifications
    - Family Members
    - Pharmacies
    - Law Enforcement (disaster relief, epidemic, etc)
- Incidental disclosures
  - Disclosure as a result of a previous disclosure

Explicitly Acceptable Disclosures

- Disclosure in Public Interest and Benefit Activities
  - Public Health (prevention or containment of a disease)
  - Employees where transmission of a dangerous disease was likely
  - Victims of abuse, neglect, violence, etc
  - Heath oversight activates and judicial proceedings

Explicitly Acceptable Disclosures

- Disclosure in Public Interest and Benefit Activities (cont'd)
  - Law enforcement purposes
  - Decedents
  - Organ, eye, tissue donations
  - Research purposes
  - Serious threat to public safety
  - … and more…

Limited Data Set

- A limited data set is PHI from which certain identifier information is removed.
  - Names; Postal address information, other than town or city, State and zip; Telephone numbers, Fax numbers; Electronic mail addresses; Social security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; Full face photographic images and any comparable images.
- Limited data set can be used for research purposes provided that the recipient of the data signs an agreement

Authorized Uses and Disclosures

- All other uses and disclosures of data but have explicit written authorization by the individual.
- Given examples:
  - Psychotherapy notes
  - Marketing
  - etc

Minimum Necessary Clause

- One of the central aspects of the entire Privacy Rule is that only the minimally necessary amount of PHI is disclosed.

“Minimum Necessary” Clause

- However, the minimum necessary clause does not cover:
  - Health care providers for treatment
  - Individuals who is the subject of the information
  - Disclosures made pursuant to an authorization
  - Disclosure to HHS or required by law
  - Disclosure for HIPAA compliance reviews

Other Privacy Rule Conditions

- Privacy Practice Notices
  - Provides the “privacy policy” of the health care institution
  - Must be easily accessible and a receipt (signature) must be on file from every patient that they had the chance to review the notice
- Patient’s right to knowledge of disclosure, with certain limitations.

Other Privacy Rule Conditions

- Confidential Communications
  - An individual may request communications be made only at a specific telephone number or a specific address.
  - Furthermore, they may request that information is sent in sealed envelopes rather than postcards or other unsecured mail

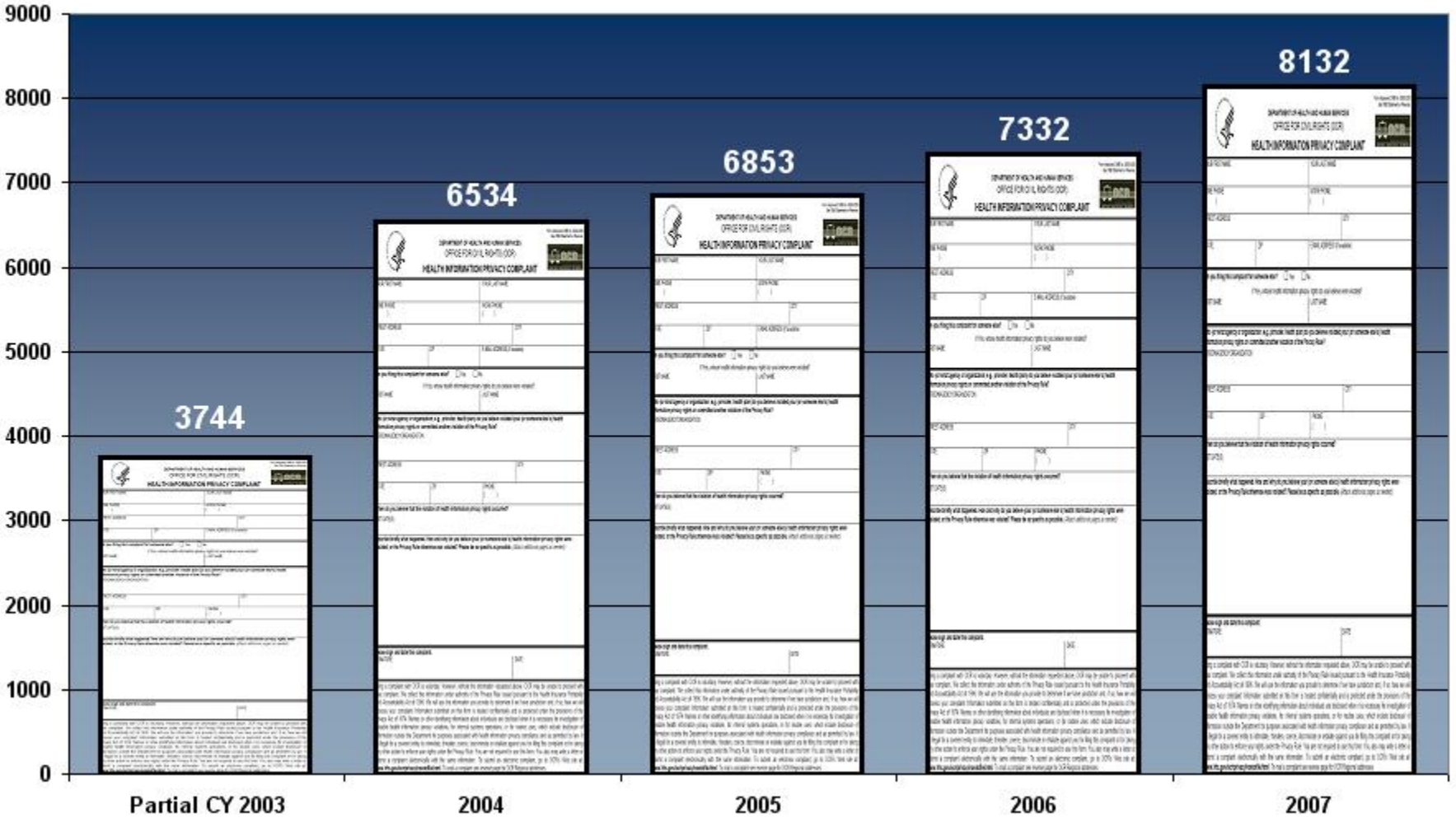
Penalties

- HHS may impose monetary civil penalties for violations of the Privacy Rule:
  - $100 per failure to comply with a Privacy Rule requirement (up to $25,000/yr/company for violations of the same Privacy Rule requirement)

Penalties

- Criminal Penalties
  - Any person (a physical person or an incorporated company) who knowingly obtains or discloses PHI is in violation of HIPAA and faces:
    - Up to a $50,000 fine
    - Up to a one-year prison term
  - An intention to sell, transfer, or use PHI increase both the fine and the prison term

Complaints related to HIPAA



Enforcement Results