

Privacy Breach Response

Professor Dorothy J. Glancy, - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment
Team for Research in Ubiquitous Secure Technology (TRUST)
June 21, 2010 Vanderbilt University, Nashville, TN

What is a Privacy Breach ?

- ◆ **Improper disclosure of personal information**
 - ◆ Without consent of the person whose information has been disclosed

- ◆ **Functionally, Personal Information leaks out**

What Counts as Personal Information ?



United States

Personal information means information that identifies an individual or can be linked to a particular identifiable individual.

Examples: Social Security Number, photograph, name, address



United Kingdom

“personal data” means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions . . . of any person in respect of the individual .

Examples: type of job you do, the things you buy and the place you went to school.



Japan

Information about a living individual, which can identify the specific individual by name, date of birth or other description.

Examples: cell phone number, passport number, photo, email address

Information Leaks . . .



Professor Dorothy Glancy - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)

June 21, 2010 Vanderbilt University, Nashville, TN

Dam Breach

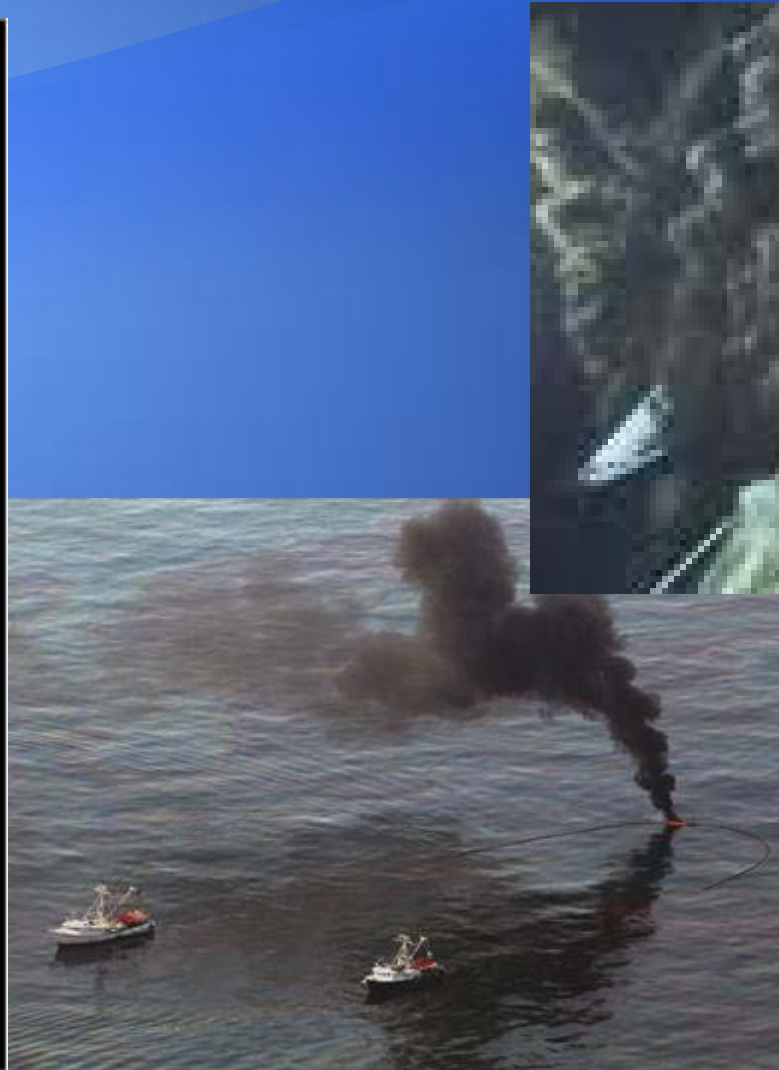


Professor Dorothy Glancy - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)

June 21, 2010 Vanderbilt University, Nashville, TN

Deep Water Horizon Blow Out



Professor Dorothy Glancy - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)

June 21, 2010 Vanderbilt University, Nashville, TN

Privacy Breach

- ◆ **Improper disclosure of personal information**
 - ◆ Without the consent of the person whose information has been disclosed
- ◆ **Personal Information leaks out**
- ◆ **And is gone!**

Or is it?

21st Century Privacy Breach Characteristics

Leaks of personal information

- ◆ About a human person
- ◆ Electronic digital data
- ◆ Kept in a database
- ◆ Containment through
 - ◆ Agreement
 - ◆ Promise
 - ◆ Law
 - ◆ Technology
 - ◆ Physical barriers
 - ◆ Intended processes

Professor Dorothy Glancy - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)

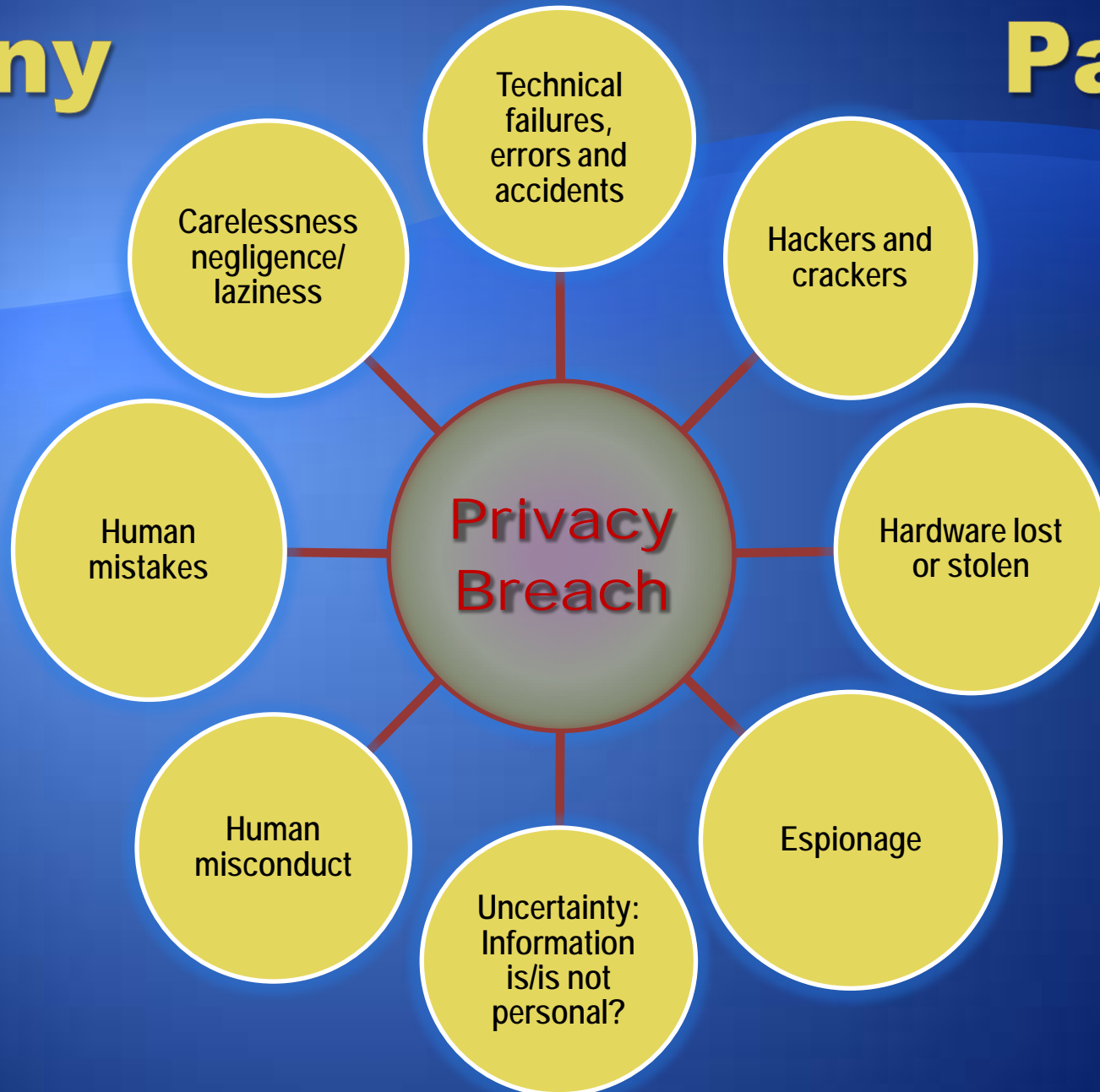
June 21, 2010 Vanderbilt University, Nashville, TN

Many Sources of Privacy Breaches

- ◆ Technical failures, errors and accidents
- ◆ Hackers and crackers
- ◆ Hardware lost or stolen
- ◆ Espionage
- ◆ Human mistakes
- ◆ Misunderstanding or disagreement about whether or not information is personal
- ◆ Human misconduct
- ◆ Carelessness - negligence/ laziness

Many

Paths



Professor Dorothy Glancy - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)

June 21, 2010 Vanderbilt University, Nashville, TN



Professor Dorothy Glancy - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)

June 21, 2010 Vanderbilt University, Nashville, TN

Consequences of Privacy Breaches

- ◆ Mostly BAD



- ◆ Unfortunate for both

- ◆ Person who leaked the personal information
- ◆ Person whose personal information was leaked

Legal Consequences of Privacy Breaches

May include:

- Notification requirements
- Monetary liability (damages)
- Criminal penalties
- Administrative action

Depending on where you are in the world
– or in cyberspace

Privacy Breach Notification Requirements



US experience

- ◆ 46 state laws require notice to person whose data was disclosed
- ◆ Federal statutes
 - ◆ Sarbanes-Oxley Act and Implementing Regulations
 - ◆ HIPPA
- ◆ Federal regulatory action
 - ◆ Federal Trade Commission
 - ◆ HHS Privacy Rule

Notification Requirements Outside the United States



◆ Europe - E-Privacy Directive

(Directive on Privacy and Electronic Communications)

- ◆ Notice to relevant national regulatory authority



◆ Asia-Pacific Economic Cooperation

- ◆ Cross-Border Privacy Rules

Monetary Liability



◆ US Court-ordered damages

◆ Statutory Damages

- ◆ E.g., under Drivers Privacy Protection Act

◆ Common Law damages

- ◆ Identity theft



◆ Japan apology payments

Administrative Sanctions



- ◆ UK Information Commissioner
 - ◆ Data Protection Act prohibits “secondary uses”



- ◆ Japan complaint process
(to relevant Ministry)



- ◆ US Federal Trade Commission enforcement
HHS Unsecured PHI Interim Final Rule
(August 2009)

Social/Reputational Sanctions



- ◆ Often monetized in the US



- ◆ In Japan, self-regulation
 - ◆ corporate responsibility to respect personal information

Responses to Privacy Breaches



Avoidance in future

- Minimization
- Anonymization
- Retention restrictions
- Robust data security

Transparency

- Publicly admit
- Report to oversight agency

Litigation

Self-regulation



Professor Dorothy Glancy - Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)

June 21, 2010 Vanderbilt University, Nashville, TN

One response does not fit every privacy breach

- ◆ Anticipation and prevention
- ◆ Social/Societal context creates expectations
- ◆ Litigation a last resort

Thank You !

Professor Dorothy J. Glancy

Santa Clara University School of Law Santa Clara, California

dglancy@scu.edu