Privacy Values and Privacy by Design

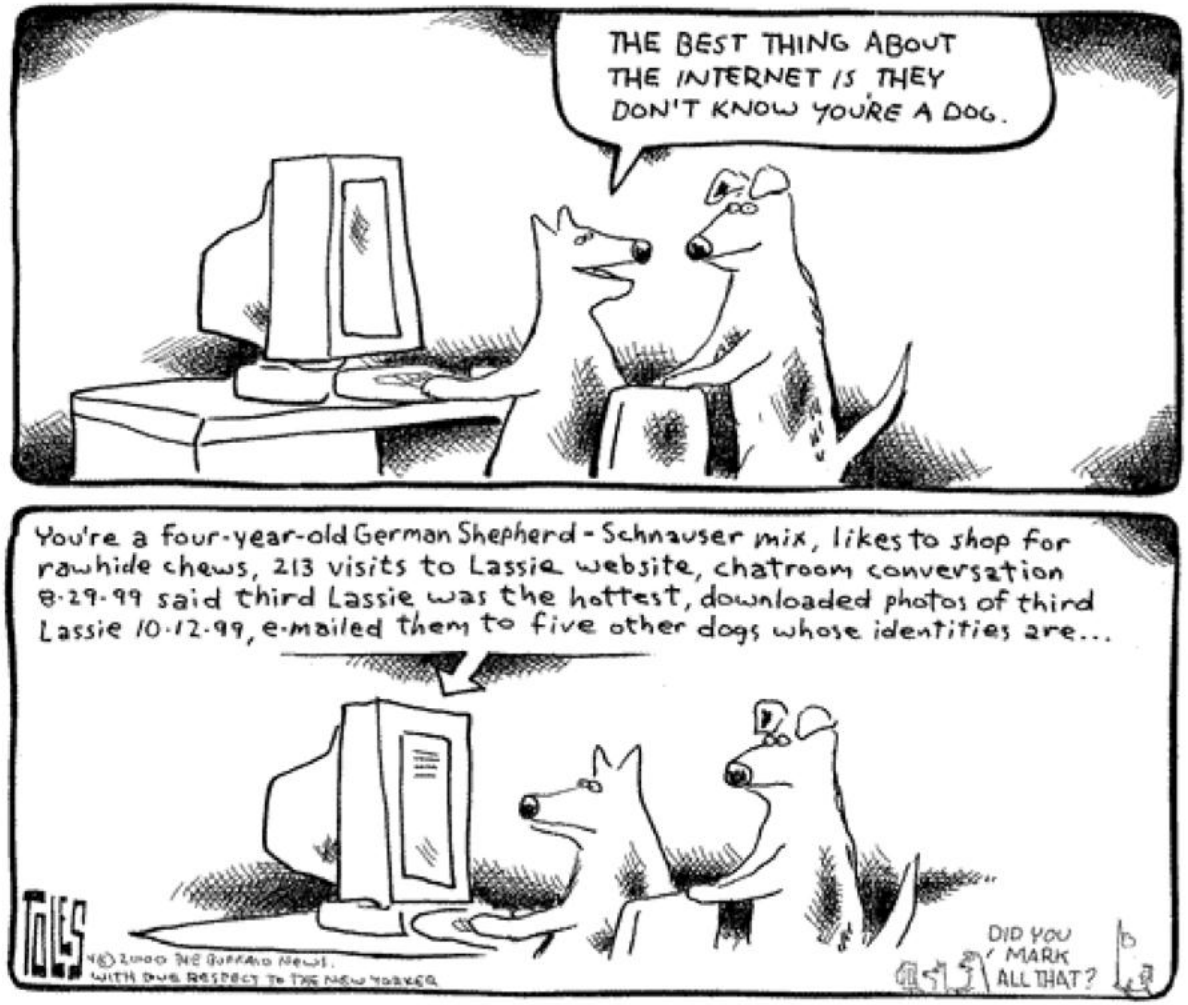
Annie I. Antón

Silicon Flatirons
The Technology of Privacy
University of Colorado School of Law
January 11, 2013

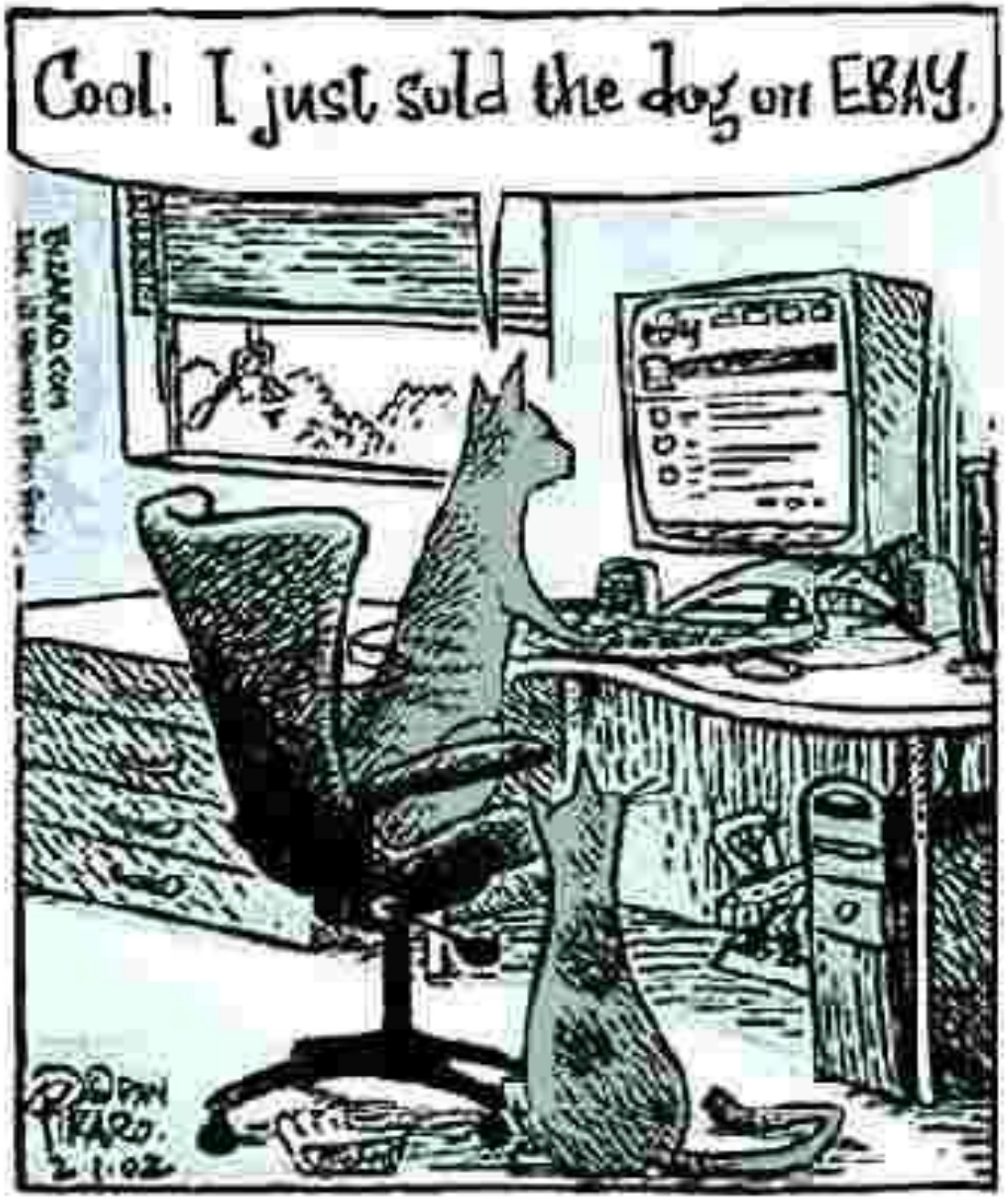
Georgia Tech College of Computing
School of Interactive Computing

the privacyplace.org

"On the Internet, nobody knows you're a dog."


THE BEST THING ABOUT THE INTERNET IS THEY DON'T KNOW YOU'RE A DOG.
You're a four-year-old German Shepherd - Schnauser mix, likes to shop for rawhide chews, 213 visits to Lassie website, chatroom conversation 8-29-99 said third Lassie was the hottest, downloaded photos of third Lassie 10-12-99, e-mailed them to five other dogs whose identities are...
TOLES
©2000 THE BUFFALO NEWS. WITH DUE RESPECT TO THE NEW YORKER
DID YOU MARK ALL THAT?

4-9-00


Cool. I just sold the dog on EBAY.
ebay
DOUG PIKARD
2.1.02

Online, how do we assure the public and what is the public concerned about?

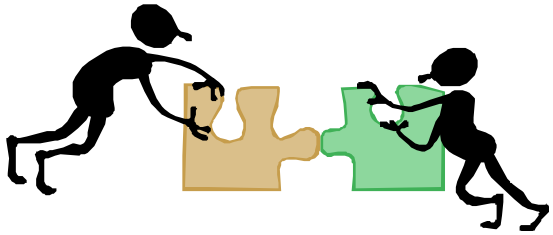
"Congratulations, Dave! I don't think I've read a more beautifully evasive and subtly misleading public statement in all my years in government."

Privacy Survey Instrument

Privacy Values Baseline Reveals Misalignment

[IEEE Trans. On Eng. Mgmt, 2005]

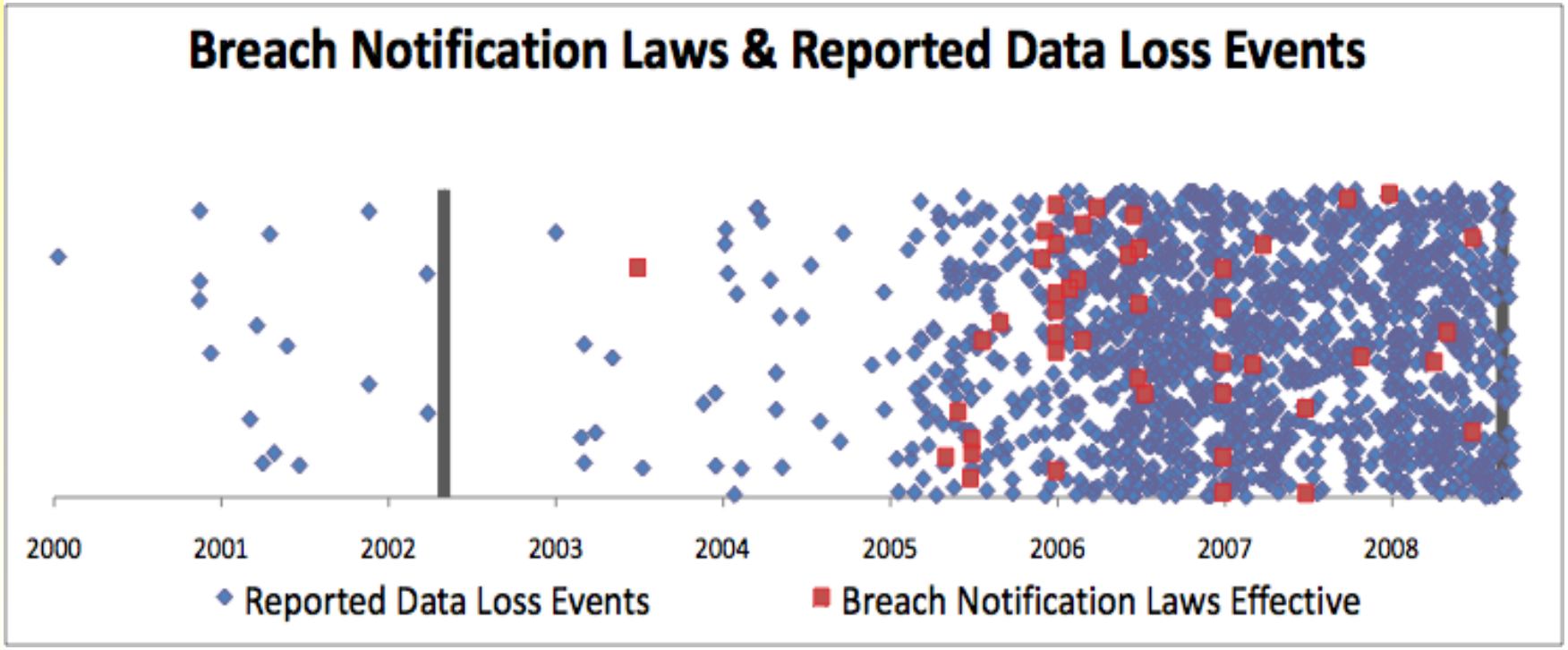
- Data was collected from 1005 Internet users in 2002 to establish a privacy values baseline for correlation with our privacy protection goals and privacy vulnerabilities taxonomy.
- Consumers are most concerned with (in order):
  - information transfer
  - notice/awareness
  - information storage
- Privacy policies emphasize (in order)
  - data integrity/security
  - information collection, and
  - user choice/consent



Georgia Tech College of Computing
School of Interactive Computing

Data losses and breach notification law since 2002 survey…

[IEEE Security & Privacy, Jan/Feb 2010]



Georgia Tech College of Computing
School of Interactive Computing

the privacyplace.org

Top privacy concerns among U.S. respondents remain the same in 2008

(1524 U.S. Respondents)

[IEEE Security & Privacy, Jan/Feb 2010]

2002 Top Concerns

- Information Transfer
- Notice & Awareness
- Information Storage

2008 Top Concerns

- Information Transfer
- Notice & Awareness
- Information Storage

Georgia Tech College of Computing
School of Interactive Computing

What has changed is individuals' level of concern …

[IEEE Security & Privacy, Jan/Feb 2010]

- Since our first survey U.S. respondents ….

Transfer

- are *more concerned* about disclosures of their purchasing patterns (p=0.0087)
- are *more concerned* about the trading/selling of PII to third parties (p=0.0013)

Notice / Aware.

- have a *stronger desire* to be notified about security safeguards being used to protect their PII (p=0.0029)
- are *less concerned* about:
  - options for deciding how their PII is used (p<0.0001)
  - changes in privacy practices (p<0.0001)
  - disclosures concerning PII use (p=0.0144)
  - previously undisclosed changes in way PII is used (p=0.0002)

Collection

- *more concerned* about websites recording information regarding previously visited web sites (p=0.0002)

US vs. Non-US Privacy Values

(1,524 U.S. and 421 Non-US Respondents)

[IEEE Security & Privacy, Jan/Feb 2010]

US Top Concerns

- Information Transfer
- Notice & Awareness
- Information Storage

Non-US Top Concerns

- Information Transfer
- Information Storage
- Notice & Awareness

Georgia Tech College of Computing
School of Interactive Computing

the privacyplace.org

Privacy by Design via Regulatory Compliance

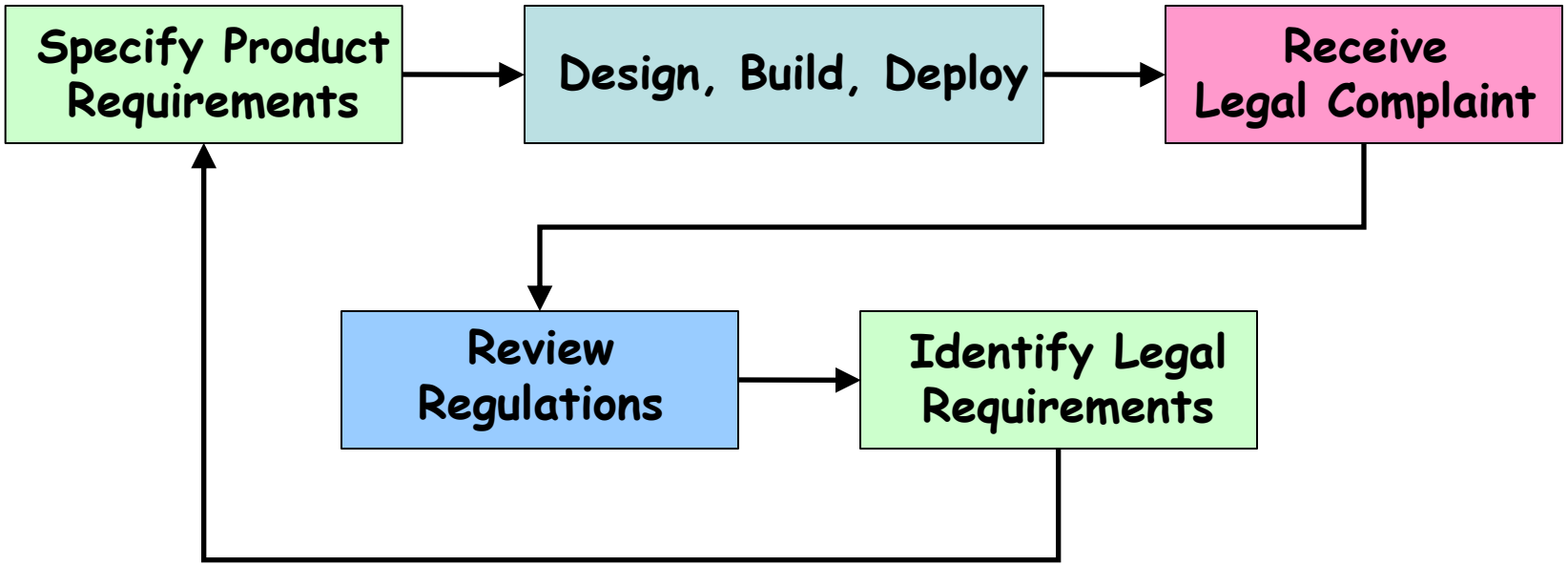
the privacyplace.org

Georgia Tech College of Computing
School of Interactive Computing

The Legal Problem

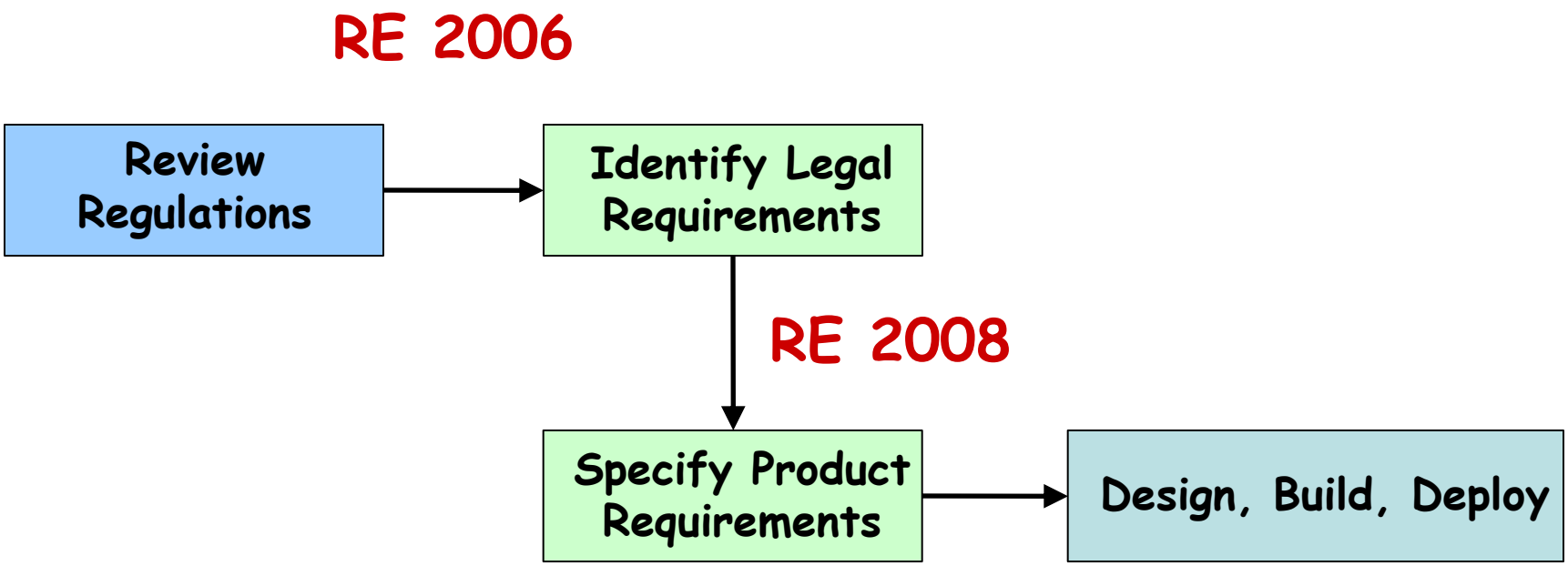
[IEEE International Requirements Conference, 2008]

- Companies must align their business practices and products requirements with government laws and regulation…



Industry Best Practice

[IEEE International Requirements Conference, 2008]



The Challenge …

- Legal cross-references introduce challenges to regulatory compliance, including: ambiguities, exceptions and conflicts.

- Requirements engineers need guidance as to how to address cross-reference to achieve compliance with legal requirements.

Compliance Goals

[IEEE TSE, January 2008]

- Due diligence refers to reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations

- Standard of care means "under the law of negligence or of obligations, the conduct demanded of a person in a situation; typically, this involves a person giving attention both to possible dangers, mistakes and pitfalls and to ways of minimizing those risks."

Black's Law Dictionary, 8th ed.

Key characteristics of legal texts

[IEEE Int'l Req'ts Eng. Conf, 2007]

- Factors that make legal texts difficult to model and use in requirements engineering and development
  - hierarchical nature of regulations
  - frequent amendments and revisions
  - cross-references: internal and external
  - definitions and acronyms
  - case law and supplemental documents
  - ambiguities: intentional and unintentional

Examples of legal ambiguity

[IEEE Int'l Req'ts Eng. Conf, 2007]

- Intentional ambiguity: HIPAA § 164.306(a)(2)

  ". . . protect against any **reasonably** anticipated threats or hazards to the security or integrity of such information"

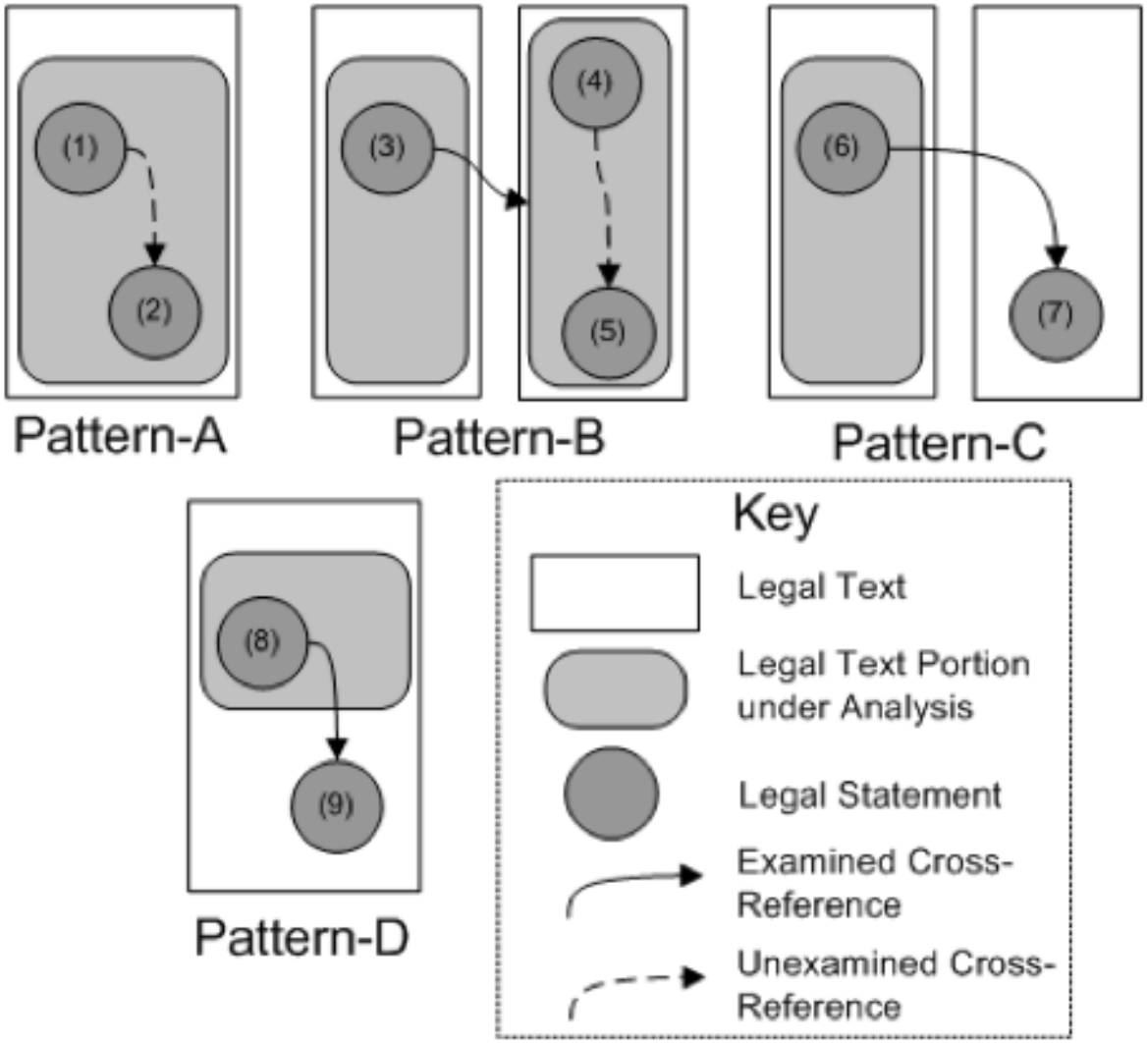
- Language ambiguity: HIPAA § 164.530(i)(3)

  ". . . the covered entity must **promptly** document **and** implement the revised policy or procedure"

Georgia Tech College of Computing
School of Interactive Computing

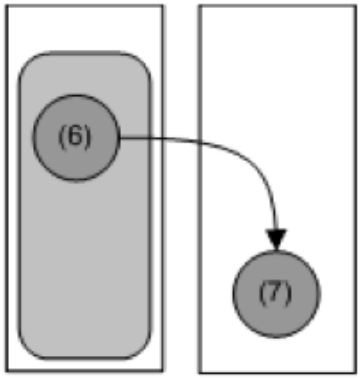
Possible Cross-References (Internal vs. External)

[IEEE Int'l Req'ts Eng. Conference, 2011]

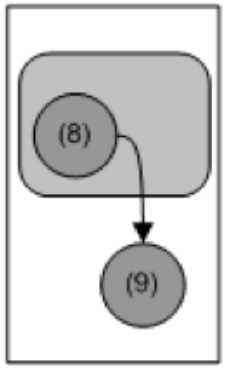


Examined External Cross-References

[IEEE Int'l Req'ts Eng. Conference, 2011]



Pattern-C



Pattern-D

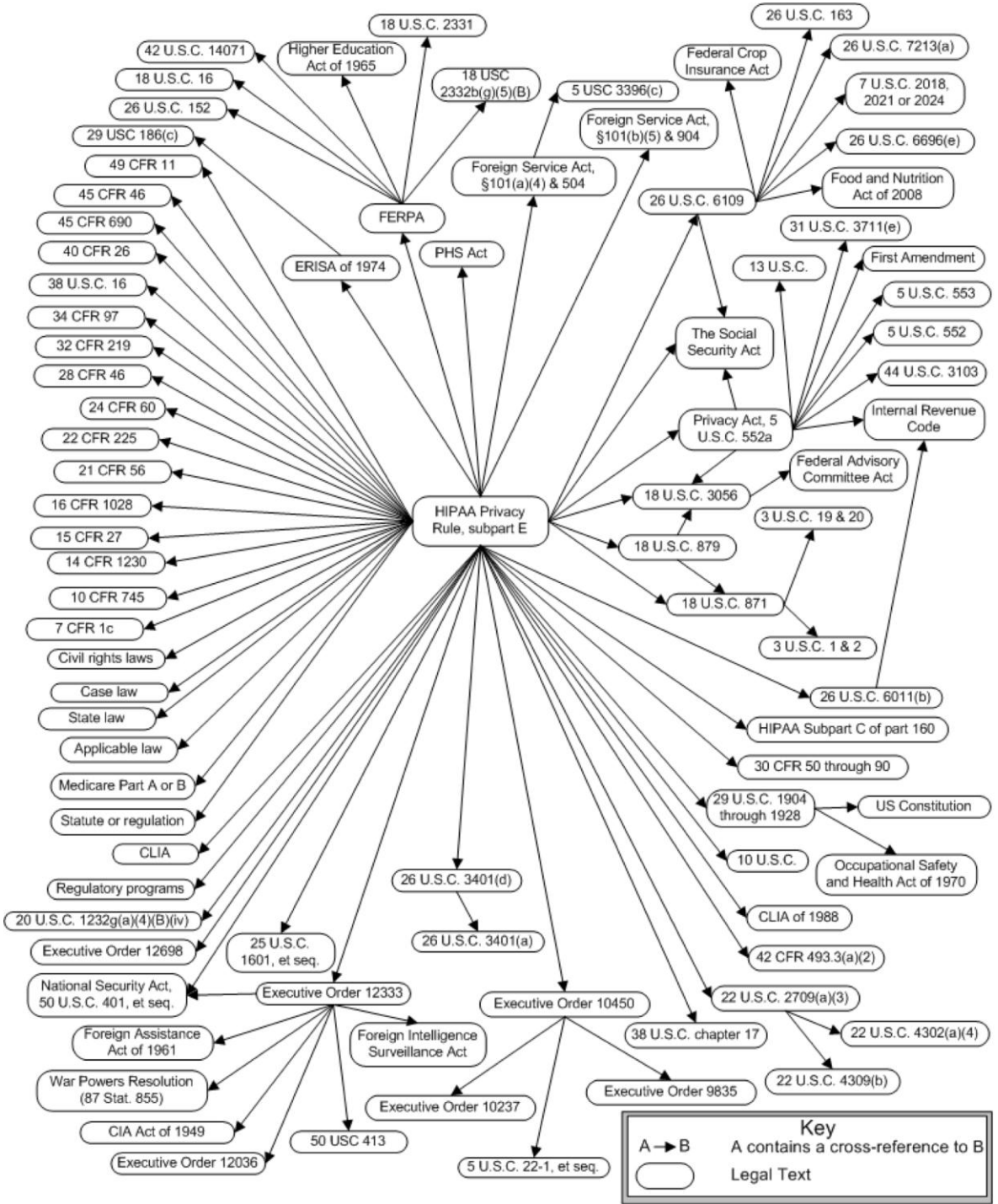
- Source Material:
  - HIPAA Privacy Rule (HPR)

    (§164.500-532 & §160.103)
- 177 examined cross-references
  - 108 cross-references in HPR

    (no more than 2 steps away from Privacy Rule)
  - 69 cross-references in referenced texts
- Approach:
  - *1st Pass:* ID'd Pattern-Cs & Pattern-Ds
  - 2nd Pass: used open coding based on cross-references' effect on compliance reqt's.

External Cross-References in the HIPAA Privacy Rule

[IEEE Int'l Req'ts Eng. Conference, 2011]



Results from Applying Legal Cross Reference Taxonomy to HIPAA

[IEEE Int'l Req'ts Eng. Conference, 2011]

Reference Type	Count
Refine	51
Exception	18
Definition	30
Unrelated	58
Incorrect	2
General	18
Total	**177**

Examining cross-references reveals conflicting requirements

- HIPAA Privacy Rule says:
  - Keep PHI for 6 years after the last use
- Privacy Act of 1974 says:
  - Keep for five years or for the life of the record

If requirements engineers focus solely on the Privacy Rule, could specify requirements that fail to comply with HIPAA.

Conflict Resolution
Strategy #1: Comply with restrictive law

[IEEE Int'l Req'ts Eng. Conference, 2011]

- Classify each legal statement as a:
  - *ceiling rule*, where the constraint is in the form "at least x", or
  - *floor rule*, where the constraint is in the form "no more than y"
- Resolve according to table

		Legal Text 1	
Legal Text 2		*Ceiling rule*	*Floor rule*
	Ceiling rule	Comply with longer time period	Consult legal domain expert
	Floor rule	Consult legal domain expert	Comply with shorter time period

Addressing Conflicts
Strategy #4: Consult Legal Domain Experts

[IEEE Int'l Req'ts Eng. Conference, 2011]

- Some conflicts may only be addressed with consultation with legal domain experts
- Example
  - HIPAA and 29 CFR 1910.1020 allow individuals & employees access to their health records
  - Both also allow covered entities and employers to deny access to health records under certain conditions
  - Conditions are mutually exclusive

Conflicting Requirements

[IEEE Int'l Req'ts Eng. Conference, 2011]

Index	Conflicting Legal Texts	Summary of Conflict	Applicable Resolution Strategies
1	• HIPAA §164.530(j)(2) • Privacy Act of 1974 (cited at §164.524(a)(2)(iv)) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Length of data retention: • HIPAA: at least 5 years • Privacy Act: at least 6 years or the life of the record, whichever is longer • 29 CFR 1910.1020: at least 30 years if the employee worked for longer than a year	• Comply with most restrictive law • Keep data separate
2	• HIPAA §164.524(b)(2) • Privacy Act of 1974 (cited at §164.524(a)(2)(iv)) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Length of time an organization has to respond to a request for access to data: • HIPAA: in fewer than 30 days • Privacy Act: in fewer than 10 days • 29 CFR 1910.1020: in fewer than 15 working days	• Comply with most restrictive law • Keep data separate
3	• HIPAA §164.524(c)(4) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Under HIPAA, a covered entity may charge a reasonable, cost-based fee when providing copies of PHI to an individual , whereas in 29 CFR 1910.1020, employers must provide the first copy of an employees medical record free of charge	• Obligations supersede legal privileges • Keep data separate
4	• HIPAA §164.524(c)(4) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	HIPAA and 29 CFR 1910.1020 contain different conditions that prevent the release of protected information to individuals. Even if an organization can withhold information under one law, they must release it under the other law.	Consult legal domain expert
5	• HIPAA §164.524(c)(4) • 29 CFR 1910.1020 (cited at §164.512(b)(1)(v)(C))	Under HIPAA, covered entities must de-identify health information before they release it, but under 29 CFR 1910.1020, they may release data to employees if personal identifiers cannot be removed.	• Do not exercise legal privileges • Keep data separate

Assessing the Accuracy of Legal Implentation Readiness Decisions

the privacyplace.org

Georgia Tech School of Interactive Computing
College of Computing

Research Goal

[IEEE Int'l Req'ts Eng. Conference, 2011]

Analyze empirical observations for the purpose of characterizing legal implementation readiness with respect to software requirements from the viewpoint of software engineers in the context of an EHR system that must comply with HIPAA regulations.

Example Non-LIR Requirement

[IEEE Int'l Req'ts Eng. Conference, 2011]

Consider Requirement B:

> iTrust shall allow an authenticated user to change their user ID and password so long as it remains unique.

[Traces to §164.312(a)(1) and §164.312(a)(2)(i)]

Relevant HIPAA Section:

(a)(1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) **Implementation specifications:** (i) **Unique user identification (Required).** Assign a unique name and/or number for identifying and tracking user identity.

Case Study Design / Materials

[IEEE Int'l Req'ts Eng. Conference, 2011]

- 32 graduate student participants
- Three experts in SWE & relevant laws/regs (1 lawyer)
  - Consensus via Wideband Delphi technique
- 8 legal requirements metrics
- 31 requirements to analyze
- Text of HIPAA §164.312
  - Focuses on Technical Measures of protection
  - Self-contained

Lessons Learned

[IEEE Int'l Req'ts Eng. Conference, 2011]

- Software engineering graduate students are ill-prepared to make legal implementation readiness decisions with any confidence.
- Subject matter experts must be involved in legal compliance decisions.
- Legal requirements metrics show potential for quickly evaluating legal compliance for software requirements.

Final Recommendations

- Ensure people who design your systems understand laws/policies and can ensure implemented systems are policy-compliant
- Legalese is ambiguous and difficult to support
  - Compliance is easier to support with formalized methods
  - Analysis exposes ambiguities and choices to thwart potential abuses or privacy breaches

Thank you!