Specifying Privacy Laws

Anupam Datta
Carnegie Mellon University
18734: Foundations of Privacy
Fall 2017
Problem Statement

Question: Is an organization’s processes and practices compliant with privacy regulations and internal policies?

▶ Examples of organizations
  ▶ Hospitals, financial institutions, universities, and other organizations that collect and use personal information

▶ Examples of privacy regulations
  ▶ Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), SB 1386
Problem Statement

**Question:** Is an organization’s processes and practices compliant with privacy regulations and internal policies?

- **Examples of organizations**
  - Hospitals, financial institutions, universities, and other organizations that collect and use personal information

- **Examples of privacy regulations**
  - Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), SB 1386

**Goal:** Develop methods and tools to aid organizations in compliance activities
Observation: Real privacy laws are complex.

- Long, dense — HIPAA Privacy Rule has 84 operational clauses for transmissions on ∼30 pages
- Too complex to be a practical day-to-day guide for Chief Privacy Officers.
Making sense of real privacy laws

Observation: Real privacy laws are complex.
  ▶ Long, dense — HIPAA Privacy Rule has 84 operational clauses for transmissions on ~30 pages
  ▶ Too complex to be a practical day-to-day guide for Chief Privacy Officers.

Desiderata: Interactive tools for enforcement and analysis
  ▶ “Are actions by Hospital Y’s employees compliant with HIPAA?”
  ▶ “Does GLBA permit Bank X to disclose Bob’s info to Charlie?”
Our Results

1. Logics for specifying privacy policies informed by the philosophical theory of contextual integrity
   (with A. Barth, J. C. Mitchell, H. Nissenbaum)
   (with H. DeYoung, D. Garg, L. Jia, D. Kaynar)
Our Results

1. Logics for specifying privacy policies informed by the philosophical theory of contextual integrity
   (with A. Barth, J. C. Mitchell, H. Nissenbaum)
   (with H. DeYoung, D. Garg, L. Jia, D. Kaynar)

2. Complete formalizations of HIPAA and GLBA’s operational requirements for transmissions
   (with H. DeYoung, D. Garg, L. Jia, D. Kaynar)
Our Results

1. Logics for specifying privacy policies informed by the philosophical theory of contextual integrity
   (with A. Barth, J. C. Mitchell, H. Nissenbaum)
   (with H. DeYoung, D. Garg, L. Jia, D. Kaynar)

2. Complete formalizations of HIPAA and GLBA’s operational requirements for transmissions
   (with H. DeYoung, D. Garg, L. Jia, D. Kaynar)

3. Automated policy monitoring with minimal human input for enforcement of HIPAA, GLBA.
   (with D. Garg, L. Jia)
Outline

Structure of privacy laws
Outline

Structure of privacy laws

Privacy Concepts
  Subjective concepts
  Mechanically Enforceable Concepts
Outline

Structure of privacy laws

Privacy Concepts

Subjective concepts
Mechanically Enforceable Concepts

Enforcement
Outline

Structure of privacy laws

Privacy Concepts
  Subjective concepts
  Mechanically Enforceable Concepts

Enforcement

Conclusion
Outline

Structure of privacy laws

Privacy Concepts
- Subjective concepts
- Mechanically Enforceable Concepts

Enforcement

Conclusion
Transmission of protected information

Transmissions of this form are governed by contextual norms (Nissenbaum 2004)
Transmission of protected information

Transmissions of this form are governed by contextual norms (Nissenbaum 2004)
Transmission of protected information

Transmissions of this form are governed by contextual norms (Nissenbaum 2004)
Transmission of protected information

Transmissions of this form are governed by contextual norms (Nissenbaum 2004)
Transmission of protected information

Transmissions of this form are governed by contextual norms (Nissenbaum 2004)
Norms of transmission in privacy laws

**Positive norms, $\varphi_i^+$:** Transmission *may occur* if condition is satisfied.

▶ “A covered entity may disclose protected health information for treatment activities [...]” [HIPAA §164.506(c)(2)]
Norms of transmission in privacy laws

**Positive norms,** $\varphi_i^+$: Transmission *may occur* if condition is satisfied.

- “A covered entity may disclose protected health information for treatment activities [...].” [HIPAA §164.506(c)(2)]

**Negative norms,** $\varphi_j^-$: Condition *must be satisfied* if transmission occurs.

- “A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes.” [HIPAA §164.508(a)(2)]
Norms of transmission in privacy laws

**Positive norms, \( \varphi_i^+ \):** Transmission *may occur* if condition is satisfied.

- “A covered entity may disclose protected health information for treatment activities [...].” [HIPAA §164.506(c)(2)]

**Negative norms, \( \varphi_j^- \):** Condition *must be satisfied* if transmission occurs.

- “A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes.” [HIPAA §164.508(a)(2)]

A transmission is lawful if and only if it satisfies at least one of the law’s positive norms and all of the law’s negative norms.

\[
maysend(p_1, p_2, m) \triangleq \left( \bigvee_i \varphi_i^+ \right) \land \left( \bigwedge_j \varphi_j^- \right)
\]
Norms of transmission in privacy laws

Positive norms, $\varphi^+_i$: Transmission may occur if condition is satisfied.

- “A covered entity may disclose protected health information for treatment activities [...].” [HIPAA §164.506(c)(2)]

Negative norms, $\varphi^-_j$: Condition must be satisfied if transmission occurs.

- “A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes.” [HIPAA §164.508(a)(2)]

A transmission is lawful if and only if it satisfies at least one of the law’s positive norms and all of the law’s negative norms.

$$maysend(p_1, p_2, m) \triangleq \left( \bigvee_i \varphi^+_i \right) \land \left( \bigwedge_j \varphi^-_j \right)$$
Norms of transmission in privacy laws

**Positive norms,** $\varphi^+_i$: Transmission *may occur* if condition is satisfied.

- “A covered entity may disclose protected health information for treatment activities [...].” [HIPAA §164.506(c)(2)]

**Negative norms,** $\varphi^-_j$: Condition *must be satisfied* if transmission occurs.

- “A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes.” [HIPAA §164.508(a)(2)]

A transmission is lawful if and only if it satisfies at least one of the law’s positive norms and all of the law’s negative norms.

$$\text{maysend}(p_1, p_2, m) \triangleq \left( \bigvee_i \varphi^+_i \right) \land \left( \bigwedge_j \varphi^-_j \right)$$
Norms of transmission in privacy laws

Positive norms, $\varphi_i^+$: Transmission may occur if condition is satisfied.

- “A covered entity may disclose protected health information for treatment activities [...]” [HIPAA §164.506(c)(2)]

Negative norms, $\varphi_j^-$: Condition must be satisfied if transmission occurs.

- “A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes.” [HIPAA §164.508(a)(2)]

A transmission is lawful if and only if it satisfies at least one of the law’s positive norms and all of the law’s negative norms.

$$\text{maysend}(p_1, p_2, m) \triangleq \left( \bigvee_i \varphi_i^+ \right) \land \left( \bigwedge_j \varphi_j^- \right)$$
Norms of transmission in privacy laws

**Positive norms,** $\varphi^+_i$: Transmission *may occur* if condition is satisfied.

- “A covered entity may disclose protected health information for treatment activities [...].” [HIPAA § 164.506(c)(2)]

**Negative norms,** $\varphi^-_j$: Condition *must be satisfied* if transmission occurs.

- “A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes.” [HIPAA § 164.508(a)(2)]

A transmission is lawful if and only if it satisfies at least one of the law’s positive norms and all of the law’s negative norms.

$maysend(p_1, p_2, m) \triangleq (\bigvee_i \varphi^+_i) \land (\bigwedge_j \varphi^-_j)$
Exceptions refine norms of transmission

**Exceptions to negative norms:**
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...].”

**Conclusion:** Satisfy either the core or one of the exceptions.

\[
\varphi_{164.508a2} \triangleq \varphi_{164.508a2} \lor (\varphi_{164.508a2iA}^e \lor \cdots)
\]
Exceptions refine norms of transmission

**Exceptions to negative norms:**
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...].”

**Conclusion:** Satisfy either the core or one of the exceptions.

$$\varphi_{164.508a2}' \triangleq \varphi_{164.508a2} \lor (\varphi_{164.508a2iA}^e \lor \cdots)$$
Exceptions refine norms of transmission

Exceptions to negative norms:
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...].”

Conclusion: Satisfy either the core or one of the exceptions.

\[ \varphi_{164.508a2}' \triangleq \varphi_{164.508a2} \lor (\varphi_{164.508a2iA} \lor \cdots) \]
Exceptions refine norms of transmission

**Exceptions to negative norms:**
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...].”

**Conclusion:** Satisfy either the core or one of the exceptions.

\[ \varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \lor (\varphi_{164.508a2iA}^e \lor \cdots) \]
Exceptions refine norms of transmission

Exceptions to negative norms:
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...].”

Conclusion: Satisfy either the core or one of the exceptions.

\[ \varphi_{164.508a2}' \triangleq \varphi_{164.508a2} \lor (\varphi_e^{164.508a2iA} \lor \cdots) \]

“Exceptions” to positive norms:
- A covered entity may disclose information to report abuse.
- Disclosures under previous require informing the victim.

Conclusion: Satisfy the core and its refinements.

\[ \varphi_{164.512c1}' \triangleq \varphi_{164.512c1} \land \varphi_e^{164.512c2} \]
Exceptions refine norms of transmission

**Exceptions to negative norms:**
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...]”

**Conclusion:** Satisfy either the core or one of the exceptions.

\[ \varphi_{164.508a2'} \triangleq \varphi_{164.508a2} \lor (\varphi_{164.508a2iA} \lor \cdots) \]

“Exceptions” to positive norms:
- A covered entity may disclose information to report abuse.
- Disclosures under previous require informing the victim.

**Conclusion:** Satisfy the core and its refinements.

\[ \varphi_{164.512c1'} \triangleq \varphi_{164.512c1} \land \varphi_{164.512c2} \]
Exceptions refine norms of transmission

Exceptions to negative norms:
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...].”

Conclusion: Satisfy either the core or one of the exceptions.

\[ \varphi_{164.508a2}^\neg \triangleq \varphi_{164.508a2}^\neg \lor (\varphi_{164.508a2A}^e \lor \cdots) \]

“Exceptions” to positive norms:
- A covered entity may disclose information to report abuse.
- Disclosures under previous require informing the victim.

Conclusion: Satisfy the core and its refinements.

\[ \varphi_{164.512c1}^+ \triangleq \varphi_{164.512c1}^+ \land \varphi_{164.512c2}^e \]
Exceptions refine norms of transmission

Exceptions to negative norms:
“A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except [...].”

Conclusion: Satisfy either the core or one of the exceptions.

\[
\varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \lor (\varphi_{164.508a2iA}^e \lor \cdots)
\]

“Exceptions” to positive norms:
- A covered entity may disclose information to report abuse.
- Disclosures under previous require informing the victim.

Conclusion: Satisfy the core and its refinements.

\[
\varphi_{164.512c1}^+ \triangleq \varphi_{164.512c1}^+ \land \varphi_{164.512c2}^e
\]
Structure of HIPAA and GLBA privacy laws

**Health Insurance Portability and Accountability Act:**
- Primarily positive norms
  - 56 positive norms, 7 negative norms, and 19 exceptions
  - Negative norms for patient consent or opt-out opportunity (§§164.508 and 164.510)
- Deny all transmissions not explicitly allowed
Structure of HIPAA and GLBA privacy laws

**Health Insurance Portability and Accountability Act:**
- Primarily positive norms
  - 56 positive norms, 7 negative norms, and 19 exceptions
  - Negative norms for patient consent or opt-out opportunity ($§§164.508$ and $164.510$)
- Deny all transmissions not explicitly allowed

**Gramm-Leach-Bliley Act:**
- Primarily negative norms
  - 5 negative norms and 10 exceptions
  - Negative norms require notices and opt-out opportunities ($§§6802$ and $6803$)
- Allow all transmissions not explicitly denied

**Important property of formalization:**
- Traceability: Each clause in the law corresponds to one norm in formalization (roughly)
Outline

Structure of privacy laws

Privacy Concepts
  Subjective concepts
  Mechanically Enforceable Concepts

Enforcement

Conclusion
Outline

Structure of privacy laws

Privacy Concepts
  Subjective concepts
  Mechanically Enforceable Concepts

Enforcement

Conclusion
Purposes of disclosures

**HIPAA §164.506(c)(2)**

“A covered entity may disclose protected health information for [the purpose of] treatment activities of a health care provider.”
Purposes of disclosures

**HIPAA §164.506(c)(2)**

“**A covered entity may disclose protected health information for [the purpose of] treatment activities of a health care provider.”**

**Conclusion:** Purpose constants and $\in_{U}$ predicate for subpurpose hierarchy
Purposes of disclosures

HIPAA §164.506(c)(2)

“A covered entity may disclose protected health information for [the purpose of] treatment activities of a health care provider.”

Conclusion: Purpose constants and $\in U$ predicate for subpurpose hierarchy

$$\varphi_{164.506c2}^+ \triangleq active\text{role}(p_1, \text{covered-entity}) \land (t \in T\phi) \land (u \in U\text{treatment}(p_2)) \land active\text{role}(p_2, \text{provider})$$
Principals’ beliefs and professional judgement

HIPAA §164.512(f)(4)

“A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement if the covered entity has a suspicion that the death may have resulted from criminal conduct.”
Principals’ beliefs and professional judgement

HIPAA §164.512(f)(4)

“A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement if the covered entity has a suspicion that the death may have resulted from criminal conduct.”

**Conclusion:** Include uninterpreted *believes*-… predicates
Principals’ beliefs and professional judgement

**HIPAA §164.512(f)(4)**

“A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement if the covered entity has a suspicion that the death may have resulted from criminal conduct.”

**Conclusion:** Include uninterpreted *believes*-... predicates

\[ \varphi_{164.512f4}^+ \triangleq \text{active role}(p_1, \text{covered-entity}) \land \\
(t \in_T \text{phi}) \land \\
\text{belong to role}(q, \text{deceased}) \land \\
\text{active role}(p_2, \text{law-enforcement-official}) \land \\
(u \in_U \text{death-notification}(q)) \land \\
\text{believes-death-may-be-result-of-crime}(p_1, q) \]
Outline

Structure of privacy laws

Privacy Concepts
  Subjective concepts
  Mechanically Enforceable Concepts

Enforcement

Conclusion
Past and future temporal requirements

**GLBA §6802(b)(1)**

“A financial institution may not disclose nonpublic personal information unless the consumer is given the opportunity to [opt-out], before the time that such information is disclosed.”
Past and future temporal requirements

**GLBA §6802(b)(1)**

“A financial institution may not disclose nonpublic personal information unless the consumer is given the opportunity to [opt-out], before the time that such information is disclosed.”

**GLBA §6803(a)**

“At the time of establishing a customer relationship and not less than annually during such relationship, a financial institution shall provide a disclosure to such customer, of such institution’s policies and practices with respect to [disclosing nonpublic personal info].”
Past and future temporal requirements

**GLBA §6802(b)(1)**

“A financial institution may not disclose nonpublic personal information unless the consumer is given the opportunity to [opt-out], before the time that such information is disclosed.”

**GLBA §6803(a)**

“At the time of establishing a customer relationship and not less than annually during such relationship, a financial institution shall provide a disclosure to such customer, of such institution’s policies and practices with respect to [disclosing nonpublic personal info].”

**Conclusion:** Borrow operators from temporal logic.
Past and future temporal requirements

**GLBA §6802(b)(1)**

“A financial institution may not disclose nonpublic personal information unless the consumer is given the opportunity to [opt-out], before the time that such information is disclosed.”

\[
\varphi_{6802b1} \triangleq \text{activerole}(p_1, \text{institution}) \land \\
(t \in T \text{ npi}) \land \\
\neg \text{activerole}(p_2, \text{affiliate}(p_1)) \land \\
\text{belongstorole}(q, \text{consumer}(p_1)) \\
\supset \\
\downarrow x. \Diamond (\downarrow y. (x - y \geq 14)) \land \\
\exists m'. \text{send}(p_1, q, m') \land \\
is\text{-notice-of-potential} \\
-\text{disclosure}(m', p_1, p_2, (q, t), u))
\]
Syntax of the Policy Logic

Objective predicates \( p_O \)
Subjective predicates \( p_S \)
Objective atoms \( P_O \) \( ::= \) \( p_O(t_1, \ldots, t_n) \)
Subjective atoms \( P_S \) \( ::= \) \( p_S(t_1, \ldots, t_n) \)
Formulas \( \alpha, \beta \) \( ::= \) \( P_O \mid P_S \mid \top \mid \bot \mid \alpha_1 \land \alpha_2 \mid \alpha_1 \lor \alpha_2 \mid \neg \alpha \mid \forall \vec{x}. (c \supset \alpha) \mid \exists \vec{x}. (c \land \alpha) \mid \downarrow x. \alpha \mid \alpha S \beta \mid \alpha U \beta \mid \Box \alpha \mid \Box \alpha \)
Restrictions \( c \) \( ::= \) \( P_O \mid \top \mid \bot \mid c_1 \land c_2 \mid c_1 \lor c_2 \mid \exists x. c \)

- Subjective predicates \( p_S \) model beliefs and purposes
- Restricted quantifiers \( \forall \vec{x}. (c \supset \alpha) \), \( \exists \vec{x}. (c \land \alpha) \)
- Temporal operators \( \downarrow x. \alpha \), \( \alpha S \beta \), \( \alpha U \beta \), \( \Box \alpha \), \( \Box \alpha \) (\( \Diamond \alpha \), \( \Diamond \alpha \) defined)
Related Work on Privacy Policy Specification

- Logics and languages for specification of privacy policies
  - P3P [Cranor et al.], XACML [OASIS], EPAL [Backes et al.], requirements engineering [Breaux and Antón], LPU [Barth et al.], Privacy APIs [Gunter et al.], deontic logic [I. Lee et al.], SecPAL [Becker et al.], ...
Related Work on Privacy Policy Specification

- Logics and languages for specification of privacy policies
  - P3P [Cranor et al.], XACML [OASIS], EPAL [Backes et al.], requirements engineering [Breaux and Antón], LPU [Barth et al.], Privacy APIs [Gunter et al.], deontic logic [I. Lee et al.], SecPAL [Becker et al.], ...

- Formal specification of privacy laws
  - LPU [Barth et al.]: Examples from HIPAA and GLBA
  - Datalog HIPAA [Lam et al.]: HIPAA §§164.502, 506, and 510
  - Privacy APIs [Gunter et al.]: HIPAA §164.506
  - Deontic logic [I. Lee et al.]: Examples from FDA CFR §610.40