

Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws

Henry DeYoung Deepak Garg Limin Jia
Dilsun Kaynar Anupam Datta

Carnegie Mellon University

Workshop on Privacy in the Electronic Society
October 4, 2010

Making sense of real privacy laws

Observation: Real privacy laws are complex.

- ▶ Examples:
 - ▶ Health Insurance Portability and Accountability Act (HIPAA)
 - ▶ Gramm-Leach-Bliley Act (GLBA)
- ▶ Long, dense — HIPAA Privacy Rule has 84 operational clauses for transmissions on ~30 pages
- ▶ Too complex to be a practical day-to-day guide.

Making sense of real privacy laws

Observation: Real privacy laws are complex.

- ▶ Examples:
 - ▶ Health Insurance Portability and Accountability Act (HIPAA)
 - ▶ Gramm-Leach-Bliley Act (GLBA)
- ▶ Long, dense — HIPAA Privacy Rule has 84 operational clauses for transmissions on ~30 pages
- ▶ Too complex to be a practical day-to-day guide.

Desiderata: Interactive tools for enforcement and analysis

- ▶ “Does GLBA permit Bank *X* to disclose Bob’s info to Charlie?”
- ▶ “Are Hospital *Y*’s policies consistent with HIPAA?”

Making sense of real privacy laws

Prior work:

- ▶ 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.], ...

Making sense of real privacy laws

Prior work:

- ▶ 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

Making sense of real privacy laws

Prior work:

- ▶ 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

Problem:

- ▶ Formalization efforts have not covered full privacy laws.
- ▶ Do these techniques scale to specification *and* computer-assisted enforcement of full privacy laws?

Our work

Contributions:

Our work

Contributions:

1. PrivacyLFP, a logic and signature for expressing privacy laws

Our work

Contributions:

1. PrivacyLFP, a logic and signature for expressing privacy laws
2. Complete formalizations of HIPAA and GLBA's operational requirements for transmissions

Our work

Contributions:

1. PrivacyLFP, a logic and signature for expressing privacy laws
2. Complete formalizations of HIPAA and GLBA's operational requirements for transmissions
3. Ambiguities in HIPAA and GLBA revealed by our formalization

Our work

Contributions:

1. PrivacyLFP, a logic and signature for expressing privacy laws
2. Complete formalizations of HIPAA and GLBA's operational requirements for transmissions
3. Ambiguities in HIPAA and GLBA revealed by our formalization
4. Preliminary ideas for enforcement of HIPAA, GLBA, etc.

Our work

Contributions:

1. PrivacyLFP, a logic and signature for expressing privacy laws
2. Complete formalizations of HIPAA and GLBA's operational requirements for transmissions
3. Ambiguities in HIPAA and GLBA revealed by our formalization
4. Preliminary ideas for enforcement of HIPAA, GLBA, etc.

Builds on the Logic of Privacy and Utility (LPU) [Barth et al.], a logical formalization of contextual integrity [Nissenbaum].

Outline

Structure of privacy laws

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

- Features with syntactic support only

- Features with semantics

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

- Features with syntactic support only

- Features with semantics

Ambiguity in GLBA's limits on redisclosure

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

- Features with syntactic support only

- Features with semantics

Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for enforcement

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

- Features with syntactic support only

- Features with semantics

Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for enforcement

Conclusion

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

- Features with syntactic support only

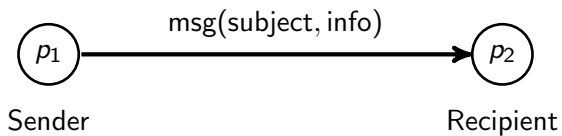
- Features with semantics

Ambiguity in GLBA's limits on redisclosure

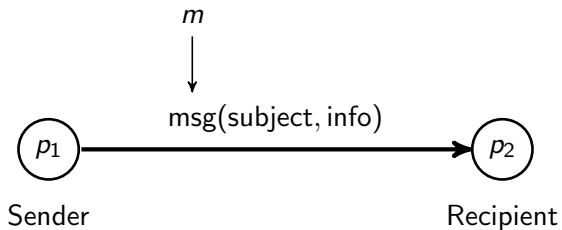
Preliminary ideas for enforcement

Conclusion

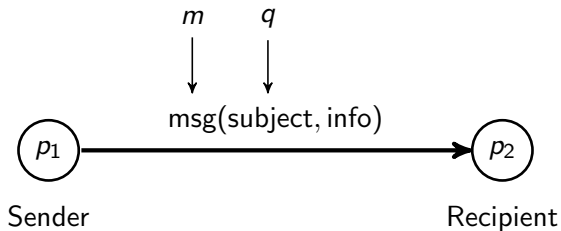
Transmission of protected information



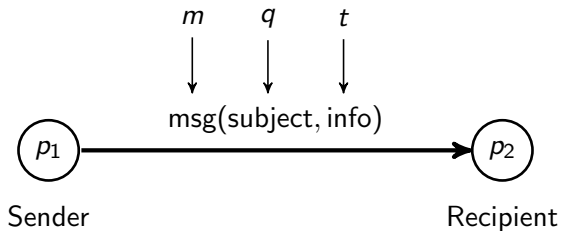
Transmission of protected information



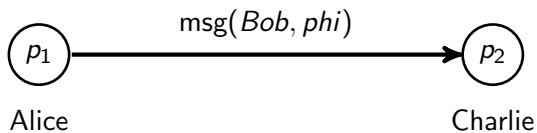
Transmission of protected information



Transmission of protected information



Transmission of protected information



Norms of transmission in privacy laws

Positive norms, φ_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, φ_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, φ_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, φ_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, φ_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.

$$\text{maysend}(p_1, p_2, m) \triangleq \left(\bigvee_i \varphi_i^+ \right) \wedge \left(\bigwedge_j \varphi_j^- \right)$$

Norms of transmission in privacy laws

Positive norms, φ_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, φ_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.

$$\text{maysend}(p_1, p_2, m) \triangleq \left(\bigvee_i \varphi_i^+ \right) \wedge \left(\bigwedge_j \varphi_j^- \right)$$

Norms of transmission in privacy laws

Positive norms, φ_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, φ_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.

$$\text{maysend}(p_1, p_2, m) \triangleq \left(\bigvee_i \varphi_i^+ \right) \wedge \left(\bigwedge_j \varphi_j^- \right)$$

Norms of transmission in privacy laws

Positive norms, φ_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, φ_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.

$$\text{maysend}(p_1, p_2, m) \triangleq \left(\bigvee_i \varphi_i^+ \right) \wedge \left(\bigwedge_j \varphi_j^- \right)$$

Norms of transmission in privacy laws

Positive norms, φ_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, φ_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**.

$$\text{maysend}(p_1, p_2, m) \triangleq \left(\bigvee_i \varphi_i^+ \right) \wedge \left(\bigwedge_j \varphi_j^- \right)$$

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.

$$\varphi_{164.508a2'}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

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.

$$\varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

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.

$$\varphi_{164.508a2'}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

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**.

$$\varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

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.

$$\varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

“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.

$$\varphi_{164.512c1}^+ \triangleq \varphi_{164.512c1}^+ \wedge \varphi_{164.512c2}^e$$

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.

$$\varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

“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.

$$\varphi_{164.512c1}^+ \triangleq \varphi_{164.512c1}^+ \wedge \varphi_{164.512c2}^e$$

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.

$$\varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

“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.

$$\varphi_{164.512c1}^+ \triangleq \varphi_{164.512c1}^+ \wedge \varphi_{164.512c2}^e$$

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.

$$\varphi_{164.508a2}^- \triangleq \varphi_{164.508a2}^- \vee (\varphi_{164.508a2iA}^e \vee \dots)$$

“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.

$$\varphi_{164.512c1}^+ \triangleq \varphi_{164.512c1}^+ \wedge \varphi_{164.512c2}^e$$

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:

- ▶ No positive norms
 - ▶ 5 negative norms and 10 exceptions
 - ▶ Negative norms require notices and opt-out opportunities (§§6802 and 6803)
- ▶ Allow all transmissions not explicitly denied

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

Features with syntactic support only

Features with semantics

Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for enforcement

Conclusion

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

Features with syntactic support only

Features with semantics

Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for 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 $\in_{\mathcal{U}}$ predicate for subpurpose hierarchy

- ▶ (*blood-tests* $\in_{\mathcal{U}}$ *treatment*) because blood tests are a type of treatment.

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 $\in_{\mathcal{U}}$ predicate for subpurpose hierarchy

- ▶ (*blood-tests* $\in_{\mathcal{U}}$ *treatment*) because blood tests are a type of treatment.

$$\varphi_{164.506c2}^+ \triangleq \text{activerole}(p_1, \text{covered-entity}) \wedge (t \in_{\mathcal{T}} \text{phi}) \wedge (u \in_{\mathcal{U}} \text{treatment}(p_2)) \wedge \text{activerole}(p_2, \text{provider})$$

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

$$\begin{aligned} \varphi_{164.512f4}^+ \triangleq & \text{activerole}(p_1, \text{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \text{phi}) \wedge \\ & \text{belongstorole}(q, \text{deceased}) \wedge \\ & \text{activerole}(p_2, \text{law-enforcement-official}) \wedge \\ & (u \in_{\mathcal{U}} \text{death-notification}(q)) \wedge \\ & \text{believes-death-may-be-result-of-crime}(p_1, q) \end{aligned}$$

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

Features with syntactic support only

Features with semantics

Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for enforcement

Conclusion

Principals' dynamic roles

Observation: Principals' roles are dynamic.

- ▶ Principals enter and exit customer relationships with banks.
- ▶ Principals are active in other roles (e.g., doctor) during customer relationship.

Principals' dynamic roles

Observation: Principals' roles are dynamic.

- ▶ Principals enter and exit customer relationships with banks.
- ▶ Principals are active in other roles (e.g., doctor) during customer relationship.

Conclusion: Distinguish the roles held from the active role.

- ▶ $belongstorole(Alice, customer(X))$: Alice is a customer of X .
- ▶ $belongstorole(Alice, doctor(Bob))$: Alice is Bob's doctor.
- ▶ $activerole(Alice, doctor(Bob))$: Alice is currently active as Bob's doctor.
- ▶ $\neg activerole(Alice, customer(X))$: Alice is *not* currently active as a customer of X .

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 and TPTL.

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 and TPTL.

- ▶ $\Diamond\phi$: “ ϕ is true at some past time.”

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 and TPTL.

- ▶ $\Diamond_{\text{past}}\phi$: “ ϕ is true at some past time.”
- ▶ $\Diamond_{\text{future}}\phi$: “ ϕ is true at some future time.”

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 and TPTL.

- ▶ $\Diamond_{\leftarrow} \phi$: “ ϕ is true at some past time.”
- ▶ $\Diamond_{\rightarrow} \phi$: “ ϕ is true at some future time.”
- ▶ $\downarrow x. \phi$: Use x as a name for the current time in ϕ .

Past and future temporal requirements

GLBA §6802(b)(1)

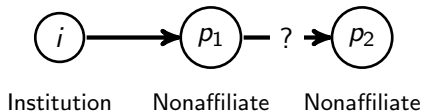
“A financial institution may not disclose nonpublic personal information unless the consumer is given the opportunity to [opt-out], **before the time that such information is disclosed.**”

$$\begin{aligned}
 \varphi_{6802b1}^- \triangleq & \text{activerole}(p_1, \text{institution}) \wedge \\
 & (t \in \mathcal{T} \text{ npi}) \wedge \\
 & \neg \text{activerole}(p_2, \text{affiliate}(p_1)) \wedge \\
 & \text{belongstorole}(q, \text{consumer}(p_1)) \\
 \rightarrow & \\
 & \downarrow x. \diamond (\downarrow y. (x - y \geq 14) \wedge \\
 & \quad \exists m'. \text{send}(p_1, q, m') \wedge \\
 & \quad \text{is-notice-of-potential} \\
 & \quad \text{-disclosure}(m', p_1, p_2, (q, t), u))
 \end{aligned}$$

Self-referential legal clauses

§6802(c) of GLBA

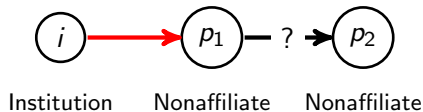
“A nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the institution.”



Self-referential legal clauses

§6802(c) of GLBA

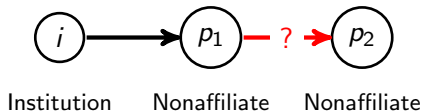
“A nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the institution.”



Self-referential legal clauses

§6802(c) of GLBA

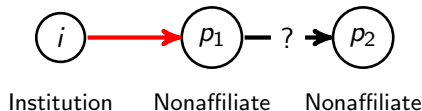
“A nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the institution.”



Self-referential legal clauses

§6802(c) of GLBA

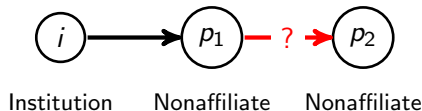
“A nonaffiliated third party **that receives nonpublic personal information from a financial institution** shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the institution.”



Self-referential legal clauses

§6802(c) of GLBA

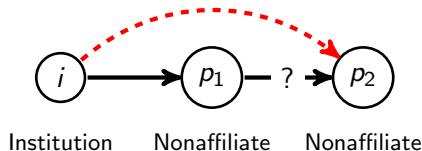
“A nonaffiliated third party that receives nonpublic personal information from a financial institution **shall not disclose such information to any other person**, unless such disclosure would be lawful if made directly to such other person by the institution.”



Self-referential legal clauses

§6802(c) of GLBA

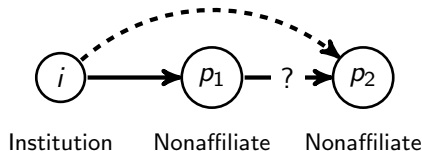
“A nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to any other person, **unless such disclosure would be lawful if made directly to such other person by the institution.**”



Self-referential legal clauses

§6802(c) of GLBA

“A nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the institution.”

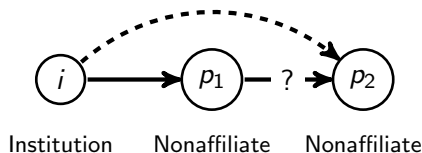


Self-referential because definition of lawful transmissions relies on the lawfulness of a hypothetical disclosure.

Self-referential legal clauses

§6802(c) of GLBA

“A nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the institution.”



Conclusion: Use recursion (fixed points) to model self-reference.

$$\nu \text{ maysend}(p_1, p_2, m). \left(\bigvee_i \varphi_i^+ \right) \wedge \left(\bigwedge_j \varphi_j^- \right)$$

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

Features with syntactic support only

Features with semantics

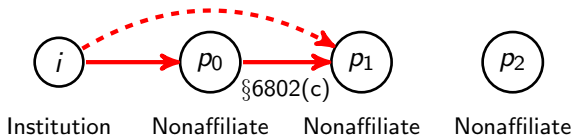
Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for enforcement

Conclusion

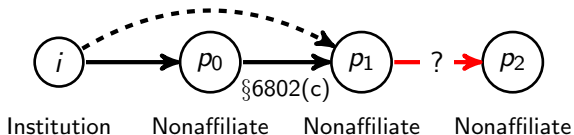
GLBA §6802(c) has short range of limits on redisclosure

Consider the scenario:



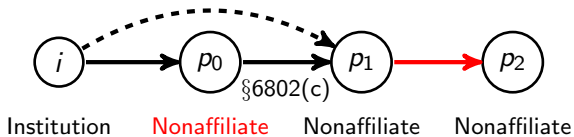
GLBA §6802(c) has short range of limits on redisclosure

Consider the scenario:



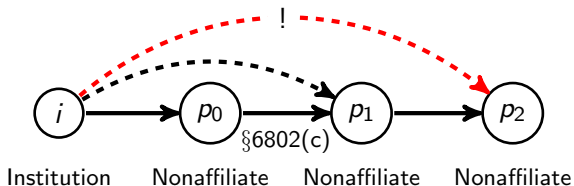
GLBA §6802(c) has short range of limits on redisclosure

Consider the scenario:



GLBA §6802(c) has short range of limits on redisclosure

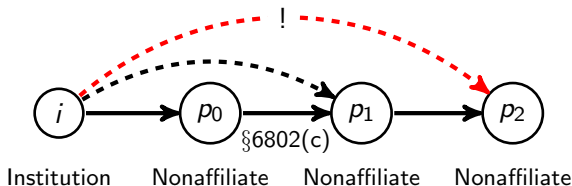
Consider the scenario:



This does not seem in the spirit of GLBA §6802(c)!

GLBA §6802(c) has short range of limits on redisclosure

Consider the scenario:

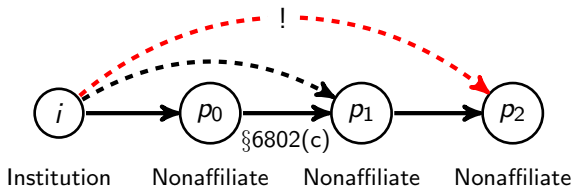


This does not seem in the spirit of GLBA §6802(c)!

Solution: Demand that the information's *origin* could legally send the information directly.

GLBA §6802(c) has short range of limits on redisclosure

Consider the scenario:



This does not seem in the spirit of GLBA §6802(c)!

Solution: Demand that the information's *origin* could legally send the information directly.

Note: Discussion of other ambiguities can be found in the paper.

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

Features with syntactic support only

Features with semantics

Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for enforcement

Conclusion

Properties of enforcement

Observations:

Enforcement by execution-time access control alone is insufficient.

- ▶ Purposes, beliefs, future obligations, etc. are not, a priori, mechanically decidable.
- ▶ Cannot always demand human involvement at execution time (e.g., medical emergency)

Properties of enforcement

Observations:

Enforcement by execution-time access control alone is insufficient.

- ▶ Purposes, beliefs, future obligations, etc. are not, a priori, mechanically decidable.
- ▶ Cannot always demand human involvement at execution time (e.g., medical emergency)

Enforcement must be:

1. execution-time access control mechanisms that may optimistically resolve undecidable predicates, postponing them to
2. post-hoc audit with human involvement.

Properties of enforcement

Observations:

Enforcement by execution-time access control alone is insufficient.

- ▶ Purposes, beliefs, future obligations, etc. are not, a priori, mechanically decidable.
- ▶ Cannot always demand human involvement at execution time (e.g., medical emergency)

Enforcement must be:

1. execution-time access control mechanisms that may optimistically resolve undecidable predicates, postponing them to
2. post-hoc audit with human involvement.

Goal: Devise decision procedures for predicates that seem mechanically undecidable.

Audit effort during enforcement

Two decision procedures:

1. Standardized data formats

- ▶ Have lawyers draft a single annual notice so that the truth of *is-annual-notice* is determined en masse for all customers.

Audit effort during enforcement

Two decision procedures:

1. Standardized data formats

- ▶ Have lawyers draft a single annual notice so that the truth of *is-annual-notice* is determined en masse for all customers.

2. Design-time analysis of business processes

- ▶ ($u \in \mathcal{U}$ *directory*) can be guaranteed true if information kiosk responds only to directory requests.

Audit effort during enforcement

Two decision procedures:

1. Standardized data formats
 - ▶ Have lawyers draft a single annual notice so that the truth of *is-annual-notice* is determined en masse for all customers.
2. Design-time analysis of business processes
 - ▶ ($u \in \mathcal{U}$ *directory*) can be guaranteed true if information kiosk responds only to directory requests.

Audit Effort	Example	Privacy Law	
		GLBA	HIPAA
None	Decision procedures	8 of 15	17 of 84

Audit effort during enforcement

Two decision procedures:

1. Standardized data formats
 - ▶ Have lawyers draft a single annual notice so that the truth of *is-annual-notice* is determined en masse for all customers.
2. Design-time analysis of business processes
 - ▶ ($u \in \mathcal{U}$ *directory*) can be guaranteed true if information kiosk responds only to directory requests.

Audit Effort	Example	Privacy Law	
		GLBA	HIPAA
None	Decision procedures	8 of 15	17 of 84
Small, non-expert	<i>prevent-fraud</i> purpose	12 of 15	47 of 84

Audit effort during enforcement

Two decision procedures:

1. Standardized data formats
 - ▶ Have lawyers draft a single annual notice so that the truth of *is-annual-notice* is determined en masse for all customers.
2. Design-time analysis of business processes
 - ▶ ($u \in \mathcal{U}$ *directory*) can be guaranteed true if information kiosk responds only to directory requests.

Audit Effort	Example	Privacy Law	
		GLBA	HIPAA
None	Decision procedures	8 of 15	17 of 84
Small, non-expert	<i>prevent-fraud</i> purpose	12 of 15	47 of 84
Large, expert	Beliefs, compliance with other laws	15 of 15	84 of 84

Audit effort during enforcement

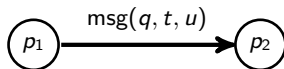
Even if experts are used for auditing, the logic **directs** their efforts.

- ▶ Only asks experts about undecidable predicates.
- ▶ Limits experts' attention to applicable positive norms, rather than the full law.

Audit effort during enforcement

Even if experts are used for auditing, the logic **directs** their efforts.

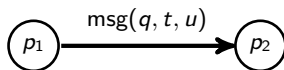
- ▶ Only asks experts about undecidable predicates.
- ▶ Limits experts' attention to applicable positive norms, rather than the full law.



Audit effort during enforcement

Even if experts are used for auditing, the logic **directs** their efforts.

- ▶ Only asks experts about undecidable predicates.
- ▶ Limits experts' attention to applicable positive norms, rather than the full law.

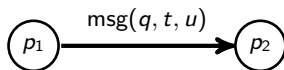


$activerole(p_1, covered-entity) \wedge$
 $activerole(p_2, law-enforcement) \wedge$
 $belongstorole(q, deceased) \wedge$
 $(t \in \mathcal{T} \text{ phi}) \wedge$
 $(u \in \mathcal{U} \text{ death-notification}(q)) \wedge$
 $believes-result-of-crime(p_1, q)$

Audit effort during enforcement

Even if experts are used for auditing, the logic **directs** their efforts.

- ▶ Only asks experts about undecidable predicates.
- ▶ Limits experts' attention to applicable positive norms, rather than the full law.



$activerole(p_1, covered-entity) \wedge$

$activerole(p_2, law-enforcement) \wedge$

$belongstorole(q, deceased) \wedge$

$(t \in_{\mathcal{T}} phi) \wedge$

$(u \in_{\mathcal{U}} death-notification(q)) \wedge$

$believes-result-of-crime(p_1, q)$

$activerole(p_1, covered-entity) \wedge$

$activerole(p_2, provider(q)) \wedge$

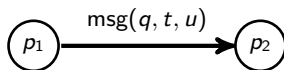
$(t \in_{\mathcal{T}} phi) \wedge$

$(u \in_{\mathcal{U}} treatment(p_2))$

Audit effort during enforcement

Even if experts are used for auditing, the logic **directs** their efforts.

- ▶ Only asks experts about undecidable predicates.
- ▶ Limits experts' attention to applicable positive norms, rather than the full law.



$activerole(p_1, covered-entity) \wedge$
 $activerole(p_2, law-enforcement) \wedge$
 $belongstorole(q, deceased) \wedge$
 $(t \in_{\mathcal{T}} phi) \wedge$
 $(u \in_{\mathcal{U}} death-notification(q)) \wedge$
 $believes-result-of-crime(p_1, q)$

~~$activerole(p_1, covered-entity) \wedge$
 $activerole(p_2, provider(q)) \wedge$
 $(t \in_{\mathcal{T}} phi) \wedge$
 $(u \in_{\mathcal{U}} treatment(p_2))$~~

Outline

Structure of privacy laws

Features of the logic PrivacyLFP

- Features with syntactic support only

- Features with semantics

Ambiguity in GLBA's limits on redisclosure

Preliminary ideas for enforcement

Conclusion

Conclusion

Contributions:

1. PrivacyLFP, a logic and signature for expressing privacy laws
 - ▶ Purposes, beliefs, dynamic roles, concrete temporal requirements, and self-referential clauses
2. Complete formalizations of HIPAA and GLBA's operational requirements for transmissions
3. Ambiguities in HIPAA and GLBA revealed by our formalization
4. Preliminary ideas for enforcement of HIPAA, GLBA, etc.

Conclusion

Contributions:

1. PrivacyLFP, a logic and signature for expressing privacy laws
 - ▶ Purposes, beliefs, dynamic roles, concrete temporal requirements, and self-referential clauses
2. Complete formalizations of HIPAA and GLBA's operational requirements for transmissions
3. Ambiguities in HIPAA and GLBA revealed by our formalization
4. Preliminary ideas for enforcement of HIPAA, GLBA, etc.

Future work:

- ▶ Enforcement!
- ▶ Semantics for de-identified data and purposes to reduce audit effort

Thank you!