Privacy Policy Specification and Enforcement: Philosophy and Law meets Computer Science

Anupam Datta

Carnegie Mellon University

CMU Privacy Research Meeting
November 23, 2010

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

Making sense of real privacy laws

Observation: Real privacy laws are complex.

- Long, dense — HIPAA Privacy Rule has 84 operational clauses for transmissions on $\sim$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 $\sim$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

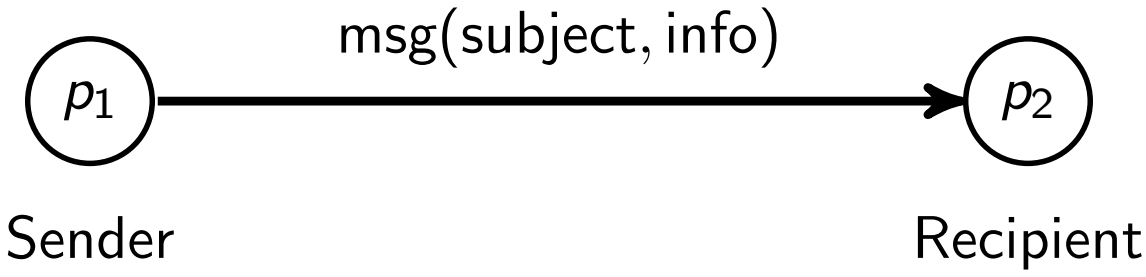
Outline

Outline

Outline

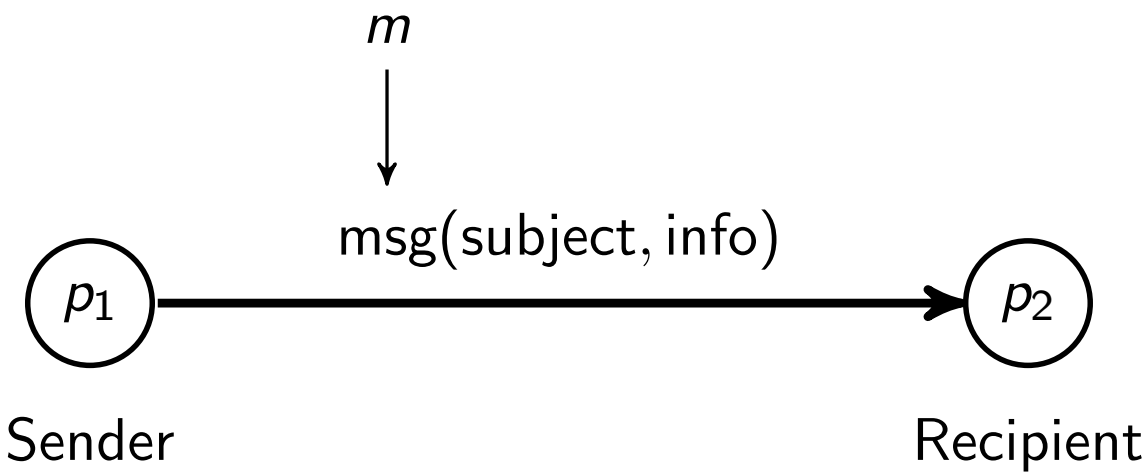
Outline

Transmission of protected information



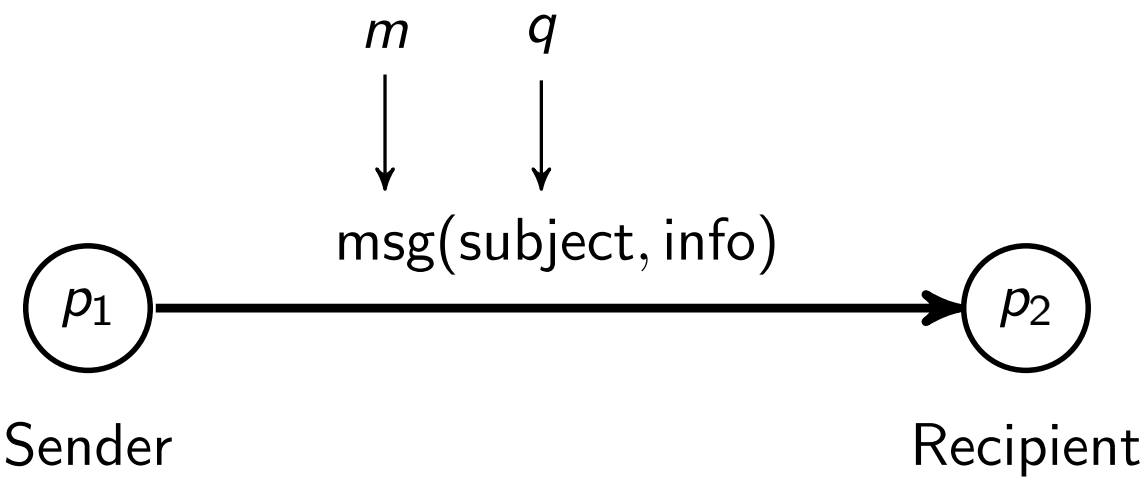
Transmissions of this form are governed by contextual norms (Nissenbaum 2004)

Transmission of protected information



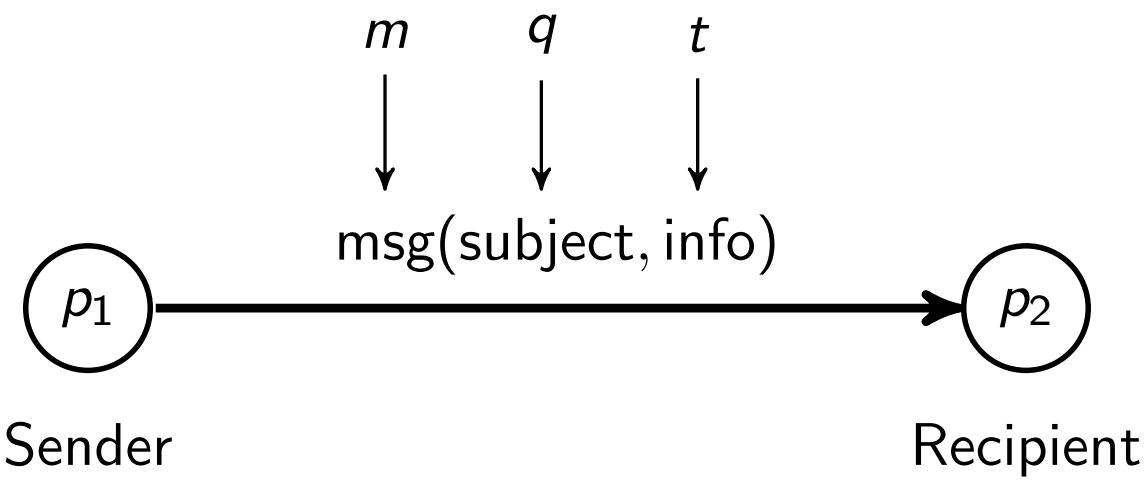
Transmissions of this form are governed by contextual norms (Nissenbaum 2004)

Transmission of protected information



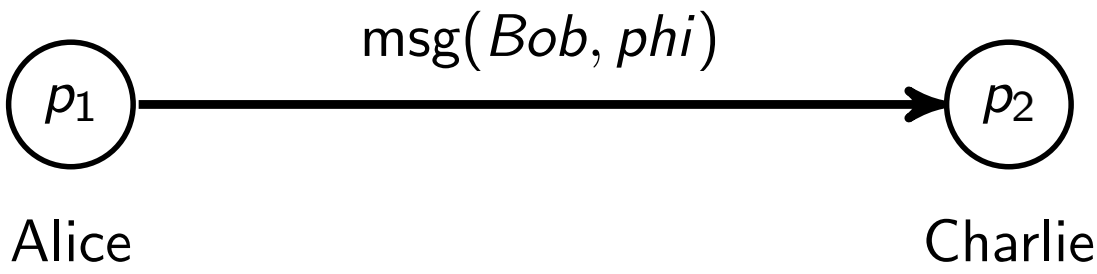
Transmissions of this form are governed by contextual norms (Nissenbaum 2004)

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, 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 satisified* 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 satisified* 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.

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

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 satisified* 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.

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

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 satisified* 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.

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

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 satisified* 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.

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

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 satisified* 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.

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

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

"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.

$$\varphi^{+}_{\texttt{164.512c1}'} \triangleq \varphi^{+}_{\texttt{164.512c1}} \wedge \varphi^{e}_{\texttt{164.512c2}}$$

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

"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.

$$\varphi^{+}_{\texttt{164.512c1}'} \triangleq \varphi^{+}_{\texttt{164.512c1}} \wedge \varphi^{e}_{\texttt{164.512c2}}$$

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

"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.

$$\varphi^{+}_{\texttt{164.512c1}'} \triangleq \varphi^{+}_{\texttt{164.512c1}} \wedge \varphi^{e}_{\texttt{164.512c2}}$$

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.

$$\varphi^{-}_{\texttt{164.508a2}'} \triangleq \varphi^{-}_{\texttt{164.508a2}} \vee (\varphi^{e}_{\texttt{164.508a2iA}} \vee \cdots)$$

"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.

$$\varphi^{+}_{\texttt{164.512c1}'} \triangleq \varphi^{+}_{\texttt{164.512c1}} \wedge \varphi^{e}_{\texttt{164.512c2}}$$

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

Outline

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

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

$$\begin{aligned}\varphi^{+}_{\texttt{164.506c2}} \triangleq\ & \mathit{activerole}(p_1, \mathit{covered\text{-}entity}) \wedge \\ & (t \in_{\mathcal{T}} \mathit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \mathit{treatment}(p_2)) \wedge \\ & \mathit{activerole}(p_2, \mathit{provider})\end{aligned}$$

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

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

Outline

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."

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

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	α, β	$::=$	$P_O \mid P_S \mid \top \mid \bot \mid$
			$\alpha_1 \wedge \alpha_2 \mid \alpha_1 \vee \alpha_2 \mid \neg\alpha \mid$
			$\forall\vec{x}.(c \supset \alpha) \mid \exists\vec{x}.(c \wedge \alpha) \mid$
			$\downarrow x.\alpha \mid \alpha\, \mathcal{S}\, \beta \mid \alpha\, \mathcal{U}\, \beta \mid \boxminus\alpha \mid \Box\, \alpha$
Restrictions	c	$::=$	$P_O \mid \top \mid \bot \mid c_1 \wedge c_2 \mid c_1 \vee c_2 \mid$
			$\exists x.c$

- Subjective predicates p_S model beliefs and purposes
- Restricted quantifiers $\forall\vec{x}.(c \supset \alpha)$, $\exists\vec{x}.(c \wedge \alpha)$
- Temporal operators $\downarrow x.\alpha$, $\alpha\, \mathcal{S}\, \beta$, $\alpha\, \mathcal{U}\, \beta$, $\boxminus\alpha$, $\Box\, \alpha$ ($\diamondminus\alpha$, $\Diamond\alpha$ 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

Outline

Properties of enforcement

Observations:

Enforcement by execution-time access control alone is insufficient.

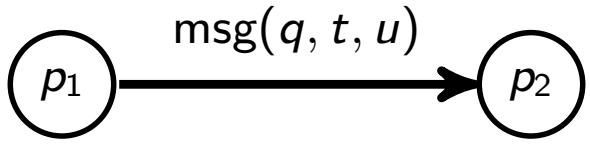
- Purposes, beliefs, future obligations, etc. are not mechanically checkable at the time of access
- Cannot always demand human involvement at execution time (e.g., medical emergency)

Enforcement of example policies

Human experts used only to resolve essential subjective predicates.

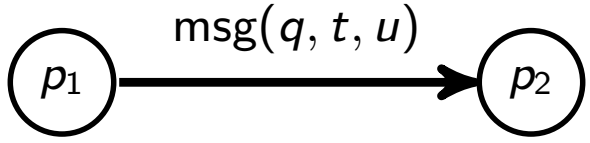
Enforcement of example policies

Human experts used only to resolve essential subjective predicates.



Enforcement of example policies

Human experts used only to resolve essential subjective predicates.



$activerole(p_1, covered\text{-}entity) \wedge$

$activerole(p_2, law\text{-}enforcement) \wedge$

$belongstorole(q, deceased) \wedge$

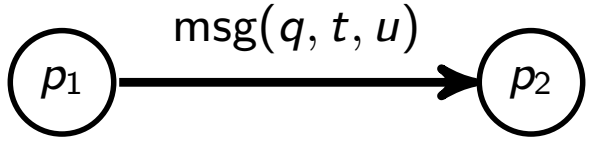
$(t \in_{\mathcal{T}} phi) \wedge$

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

$believes\text{-}result\text{-}of\text{-}crime(p_1, q)$

Enforcement of example policies

Human experts used only to resolve essential subjective predicates.



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

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

Policy Monitoring Algorithm

- Checks as much policy as possible over audit log and outputs a residual policy:

$$\texttt{reduce}(L, \varphi) = \varphi'$$

Policy Monitoring Algorithm

- Checks as much policy as possible over audit log and outputs a residual policy:

$$\texttt{reduce}(L, \varphi) = \varphi'$$

- Applied iteratively as log records more actions:

$$\begin{aligned}\texttt{reduce}(L_1, \varphi_0) &= \varphi_1\\ \texttt{reduce}(L_2, \varphi_1) &= \varphi_2\\ \ldots\end{aligned}$$

Policy Monitoring Algorithm

- Checks as much policy as possible over audit log and outputs a residual policy:

$$\texttt{reduce}(L, \varphi) = \varphi'$$

- Applied iteratively as log records more actions:

$$\texttt{reduce}(L_1, \varphi_0) = \varphi_1$$
$$\texttt{reduce}(L_2, \varphi_1) = \varphi_2$$
$$\ldots$$

- Properties
  - Sound: Any extension of log satisfies residual policy iff it satisfies original policy

Policy Monitoring Algorithm

- Checks as much policy as possible over audit log and outputs a residual policy:

$$\texttt{reduce}(L, \varphi) = \varphi'$$

- Applied iteratively as log records more actions:

$$\texttt{reduce}(L_1, \varphi_0) = \varphi_1$$
$$\texttt{reduce}(L_2, \varphi_1) = \varphi_2$$
$$\ldots$$

- Properties
  - Sound: Any extension of log satisfies residual policy iff it satisfies original policy
  - Minimal: Residual policy contains only those predicates whose truth cannot be determined from the current log (e.g., future obligations, subjective predicates)

Simpler Sublogic

$$
\begin{array}{lrcl}
\text{Formulas} & \varphi & ::= & P_O \mid P_S \mid \top \mid \bot \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \\
 & & & \forall \vec{x}.(c \supset \varphi) \mid \exists \vec{x}.(c \wedge \varphi) \\
 & & & \\
\text{Restrictions} & c & ::= & P_O \mid \top \mid \bot \mid c_1 \wedge c_2 \mid c_1 \vee c_2 \mid \\
 & & & \exists x.c
\end{array}
$$

- Policy logic with temporal operators translated into sublogic

Modeling Incomplete Audit Logs

- Structures L model audit logs with possibly *incomplete information*
- Map each atom to $\mathtt{tt}$ (true), $\mathtt{ff}$ (false), $\mathtt{uu}$ (unknown)

$$\rho_L(P) \in \{\mathtt{tt}, \mathtt{ff}, \mathtt{uu}\}$$

Modeling Incomplete Audit Logs

- Structures L model audit logs with possibly *incomplete information*
- Map each atom to $\mathtt{tt}$ (true), $\mathtt{ff}$ (false), $\mathtt{uu}$ (unknown)

$$\rho_L(P) \in \{\mathtt{tt}, \mathtt{ff}, \mathtt{uu}\}$$

- Incompleteness in practice
  - Subjective incompleteness (log lacks subjective knowledge)

Modeling Incomplete Audit Logs

- Structures L model audit logs with possibly *incomplete information*
- Map each atom to $\mathtt{tt}$ (true), $\mathtt{ff}$ (false), $\mathtt{uu}$ (unknown)

$$\rho_L(P) \in \{\mathtt{tt}, \mathtt{ff}, \mathtt{uu}\}$$

- Incompleteness in practice
  - Subjective incompleteness (log lacks subjective knowledge)
  - Future incompleteness (log does not predict the future)

Modeling Incomplete Audit Logs

- Structures L model audit logs with possibly *incomplete information*
- Map each atom to $\mathtt{tt}$ (true), $\mathtt{ff}$ (false), $\mathtt{uu}$ (unknown)

$$\rho_L(P) \in \{\mathtt{tt}, \mathtt{ff}, \mathtt{uu}\}$$

- Incompleteness in practice
  - Subjective incompleteness (log lacks subjective knowledge)
  - Future incompleteness (log does not predict the future)
  - Past incompleteness (log may miss relevant past states)

Modeling Incomplete Audit Logs

- Structures L model audit logs with possibly *incomplete information*
- Map each atom to $\mathtt{tt}$ (true), $\mathtt{ff}$ (false), $\mathtt{uu}$ (unknown)

$$\rho_L(P) \in \{\mathtt{tt}, \mathtt{ff}, \mathtt{uu}\}$$

- Incompleteness in practice
  - Subjective incompleteness (log lacks subjective knowledge)
  - Future incompleteness (log does not predict the future)
  - Past incompleteness (log may miss relevant past states)
  - Spatial incompleteness (log lacks knowledge at remote sites)

Modeling Incomplete Audit Logs

- Structures L model audit logs with possibly *incomplete information*
- Map each atom to $\mathtt{tt}$ (true), $\mathtt{ff}$ (false), $\mathtt{uu}$ (unknown)

$$\rho_L(P) \in \{\mathtt{tt}, \mathtt{ff}, \mathtt{uu}\}$$

- Incompleteness in practice
  - Subjective incompleteness (log lacks subjective knowledge)
  - Future incompleteness (log does not predict the future)
  - Past incompleteness (log may miss relevant past states)
  - Spatial incompleteness (log lacks knowledge at remote sites)
- Log evolution modeled as a relation $L' \geq L$

$$(\rho_L(P) \in \{\mathtt{tt}, \mathtt{ff}\}) \Rightarrow (\rho_{L'}(P) = \rho_L(P))$$

Reduction Algorithm

$$\texttt{reduce}(L, P) \quad = \quad \begin{cases} \top & \text{if } \rho_L(P) = \texttt{tt} \\ \bot & \text{if } \rho_L(P) = \texttt{ff} \\ P & \text{if } \rho_L(P) = \texttt{uu} \end{cases}$$

Reduction Algorithm

$$\texttt{reduce}(L, P) = \begin{cases} \top & \text{if } \rho_L(P) = \texttt{tt} \\ \bot & \text{if } \rho_L(P) = \texttt{ff} \\ P & \text{if } \rho_L(P) = \texttt{uu} \end{cases}$$

$$\texttt{reduce}(L, \varphi_1 \wedge \varphi_2) = \texttt{reduce}(L, \varphi_1) \wedge \texttt{reduce}(L, \varphi_2)$$

Reduction Algorithm

$$\texttt{reduce}(L, P) = \begin{cases} \top & \text{if } \rho_L(P) = \texttt{tt} \\ \bot & \text{if } \rho_L(P) = \texttt{ff} \\ P & \text{if } \rho_L(P) = \texttt{uu} \end{cases}$$

$$\texttt{reduce}(L, \varphi_1 \wedge \varphi_2) = \texttt{reduce}(L, \varphi_1) \wedge \texttt{reduce}(L, \varphi_2)$$

$$\begin{aligned} \texttt{reduce}(L, \forall \vec{x}.(c \supset \varphi)) = \ & \text{let} \\ & \{\sigma_1, \ldots, \sigma_n\} \leftarrow \widehat{\texttt{sat}}(L, c) \\ & \{\vec{t_i} \leftarrow \sigma_i(\vec{x})\}_{i=1}^{n} \\ & S \leftarrow \{\vec{t_1}, \ldots, \vec{t_n}\} \\ & \{\psi_i \leftarrow \texttt{reduce}(L, \varphi[\vec{t_i}/\vec{x}])\}_{i=1}^{n} \\ & \psi' \leftarrow \forall \vec{x}.((c \wedge \vec{x} \notin S) \supset \varphi) \\ & \text{return} \\ & \quad \psi_1 \wedge \ldots \wedge \psi_n \wedge \psi' \end{aligned}$$

Reduction Example

- Policy $\varphi = \forall p_1, p_2, m.\ (\mathit{send}(p_1, p_2, m) \supset \mathit{is\_law\_official}(p_2))$

Reduction Example

- Policy $\varphi = \forall p_1, p_2, m.\ (\mathit{send}(p_1, p_2, m) \supset \mathit{is\_law\_official}(p_2))$
- Structure L contains two message transmissions:
  - $\mathit{send}(A, B, M_1)$
  - $\mathit{send}(C, D, M_2)$

Reduction Example

- Policy $\varphi = \forall p_1, p_2, m.\ (\mathit{send}(p_1, p_2, m) \supset \mathit{is\_law\_official}(p_2))$
- Structure L contains two message transmissions:
  - $\mathit{send}(A, B, M_1)$
  - $\mathit{send}(C, D, M_2)$
- Reduction yields $\texttt{reduce}(L, \varphi) = \psi$, where

$$
\begin{aligned}
\psi \quad = \quad & \mathit{is\_law\_official}(B) \wedge \\
& \mathit{is\_law\_official}(D) \wedge \\
& \forall p_1, p_2, m.\ ((\mathit{send}(p_1, p_2, m) \wedge \\
& \qquad (p_1, p_2, m) \notin \{(A, B, M_1), (C, D, M_2)\}) \\
& \qquad \supset \mathit{is\_law\_official}(p_2))
\end{aligned}
$$

Special Case: Models of Temporal Logic

- Audit log complete up to current time

Special Case: Models of Temporal Logic

- Audit log complete up to current time
- Enforce safety properties at the earliest

Special Case: Models of Temporal Logic

- Audit log complete up to current time
- Enforce safety properties at the earliest
- Safety property: "A bad state is never reached"

Special Case: Models of Temporal Logic

- Audit log complete up to current time
- Enforce safety properties at the earliest
- Safety property: "A bad state is never reached"

  "Any violation of a safety property can be detected in the next reduction"

Theorem (Enforcement of safety properties)

Suppose φ is a safety property and L is complete up to time τ_0. Then, $\texttt{reduce}(L, \varphi) \rightarrow^* \bot$ if and only if there is a time $\tau \leq \tau_0$ at which φ has been violated.

Application to HIPAA

- HIPAA: 84 clauses in all

Application to HIPAA

- HIPAA: 84 clauses in all
- 17 clauses are safety properties
  - Mechanically enforcable (previous theorem)

Application to HIPAA

- HIPAA: 84 clauses in all
- 17 clauses are safety properties
  - Mechanically enforcable (previous theorem)
- 67 clauses are safety properties with subjective predicates
  - Simplify to conjunctions and disjunctions of subjective predicates through `reduce`

Related Work on Policy Enforcement

- All existing work assumes temporal logs
- Does not consider subjective predicates

Related Work on Policy Enforcement

- All existing work assumes temporal logs
- Does not consider subjective predicates
- Policy monitoring in Metric First-order Temporal Logic (MFOTL) [Basin et al'10]
  - State-of-the-art policy monitoring algorithm
  - Bounded temporal operators
  - Restrictive first-order quantification; cannot express many HIPAA clauses
  - No intermediate reducts: waits till log sufficiently complete
  - Substantial implementation and evaluation effort

Related Work on Policy Enforcement

- All existing work assumes temporal logs
- Does not consider subjective predicates
- Policy monitoring in Metric First-order Temporal Logic (MFOTL) [Basin et al'10]
  - State-of-the-art policy monitoring algorithm
  - Bounded temporal operators
  - Restrictive first-order quantification; cannot express many HIPAA clauses
  - No intermediate reducts: waits till log sufficiently complete
  - Substantial implementation and evaluation effort
- Iterative policy reduction [Roşu et al'05]
  - No quantification

Related Work on Policy Enforcement

- All existing work assumes temporal logs
- Does not consider subjective predicates
- Policy monitoring in Metric First-order Temporal Logic (MFOTL) [Basin et al'10]
  - State-of-the-art policy monitoring algorithm
  - Bounded temporal operators
  - Restrictive first-order quantification; cannot express many HIPAA clauses
  - No intermediate reducts: waits till log sufficiently complete
  - Substantial implementation and evaluation effort
- Iterative policy reduction [Roşu et al'05]
  - No quantification

Outline

Conclusion: Specification

- Logics for specifying privacy policies informed by the philosophical theory of contextual integrity

Conclusion: Specification

- Logics for specifying privacy policies informed by the philosophical theory of contextual integrity
  - Norms of transmission of personal information, composition of norms, exceptions

Conclusion: Specification

- Logics for specifying privacy policies informed by the philosophical theory of contextual integrity
  - Norms of transmission of personal information, composition of norms, exceptions
- Complete formalizations of HIPAA and GLBA's operational requirements for transmissions

Conclusion: Specification

- Logics for specifying privacy policies informed by the philosophical theory of contextual integrity
  - Norms of transmission of personal information, composition of norms, exceptions
- Complete formalizations of HIPAA and GLBA's operational requirements for transmissions
  - Subjective concepts (beliefs, purposes), real-time temporal properties (consent, notice, response), quantification over infinite domains (messages, principals)

Conclusion: Specification

- Logics for specifying privacy policies informed by the philosophical theory of contextual integrity
  - Norms of transmission of personal information, composition of norms, exceptions
- Complete formalizations of HIPAA and GLBA's operational requirements for transmissions
  - Subjective concepts (beliefs, purposes), real-time temporal properties (consent, notice, response), quantification over infinite domains (messages, principals)
  - Formalized all 84 transmission-related clauses from HIPAA Privacy Rule

Conclusion: Enforcement

- Automated policy monitoring with minimal human input for enforcement of HIPAA, GLBA

Conclusion: Enforcement

- Automated policy monitoring with minimal human input for enforcement of HIPAA, GLBA
  - Technical challenges stem from subjective predicates, real-time temporal properties, and quantification over infinite domains

Conclusion: Enforcement

- Automated policy monitoring with minimal human input for enforcement of HIPAA, GLBA
  - Technical challenges stem from subjective predicates, real-time temporal properties, and quantification over infinite domains
  - Partial structures: Logs are incomplete and they evolve (trace models for temporal logic are a special case)

Conclusion: Enforcement

- Automated policy monitoring with minimal human input for enforcement of HIPAA, GLBA
  - Technical challenges stem from subjective predicates, real-time temporal properties, and quantification over infinite domains
  - Partial structures: Logs are incomplete and they evolve (trace models for temporal logic are a special case)
  - Residual policy is minimal: contains predicates that cannot be determined from the log (subjective predicates, future obligations)

Conclusion: Enforcement

- Automated policy monitoring with minimal human input for enforcement of HIPAA, GLBA
  - Technical challenges stem from subjective predicates, real-time temporal properties, and quantification over infinite domains
  - Partial structures: Logs are incomplete and they evolve (trace models for temporal logic are a special case)
  - Residual policy is minimal: contains predicates that cannot be determined from the log (subjective predicates, future obligations)
  - Fully automated enforcement of 17 clauses from the HIPAA Privacy Rule; minimal human input for other 67.

Ongoing Work

- Implementation and evaluation of policy monitoring algorithm
  (with D. Garg, L. Jia)

Ongoing Work

- Implementation and evaluation of policy monitoring algorithm
  (with D. Garg, L. Jia)
- Audit mechanisms based on techniques from online learning theory that guide human audit
  (with J. Blocki, N. Christin, A. Sinha)

Ongoing Work

- Implementation and evaluation of policy monitoring algorithm
  (with D. Garg, L. Jia)
- Audit mechanisms based on techniques from online learning theory that guide human audit
  (with J. Blocki, N. Christin, A. Sinha)
- Semantic definition and enforcement techniques for "use-purpose" policies
  (with M. C. Tschantz, J. M. Wing)

Thank you!

Semantics of the Sublogic

$L \models P$ iff $\rho_L(P) = \mathtt{tt}$

$L \models \top$

$L \models \varphi \wedge \psi$ iff $L \models \varphi$ and $L \models \psi$

$L \models \varphi \vee \psi$ iff $L \models \varphi$ or $L \models \psi$

$L \models \forall \vec{x}.(c \supset \varphi)$ iff for all $\vec{t}$ either $L \models \overline{c}[\vec{t}/\vec{x}]$ or $L \models \varphi[\vec{t}/\vec{x}]$

$L \models \exists \vec{x}.(c \wedge \varphi)$ iff there exists $\vec{t}$ such that $L \models c[\vec{t}/\vec{x}]$ and $L \models \varphi[\vec{t}/\vec{x}]$

Definition of $\widehat{sat}$

Assume: The function $\mathtt{sat}(L, P)$ computes all substitutions σ for variables in P such that $L \models P\sigma$, if certain argument positions in P are ground.

$$
\begin{array}{lcl}
\widehat{\mathtt{sat}}(L, p_O(t_1, \ldots, t_n)) & = & \mathtt{sat}(L, p_O(t_1, \ldots, t_n)) \\
\widehat{\mathtt{sat}}(L, \top) & = & \{\bullet\} \\
\widehat{\mathtt{sat}}(L, \bot) & = & \{\} \\
\widehat{\mathtt{sat}}(L, c_1 \wedge c_2) & = & \bigcup_{\sigma \in \widehat{\mathtt{sat}}(L, c_1)} \sigma + \widehat{\mathtt{sat}}(L, c_2\sigma) \\
\widehat{\mathtt{sat}}(L, c_1 \vee c_2) & = & \widehat{\mathtt{sat}}(L, c_1) \cup \widehat{\mathtt{sat}}(L, c_2) \\
\widehat{\mathtt{sat}}(L, \exists x.c) & = & \widehat{\mathtt{sat}}(L, c) \backslash \{x\} \qquad (x \text{ fresh})
\end{array}
$$