Representing Policy for Enterprise Compliance

NIST Privilege Management Workshop

Plenary Session

September 1, 2009

K. Krasnow Waterman

LawTechIntersect, LLC

Speaker Bio

- Present:
  - Law & Technology consultant
  - Visiting Fellow, Massachusetts Institute of Technology, Decentralized Information Group, Computer Science & Artificial Intelligence Lab
  - Co-Chair, Artificial Intelligence Committee, American Bar Association
- Past
  - CIO, Foreign Terrorist Tracking Task Force
  - Section Chief (interim), Intelligence Infrastructure, FBI
  - Assistant General Counsel, FBI
- Dual Degrees - Law and Management of Technology

Policy

- Multiple documents mandate when and how data should be accessed, retained, manipulated, shared, and destroyed
  - Law
  - Regulation
  - Contract
  - MOU
  - Organizational policy
  - Counsel opinion

Legal Policies

- Typically address
  - Persons/entities
  - Data
  - Action
  - Context/Circumstances

Past

- Handled compliance *outside* enterprise systems.
  - Human determination that a person met criteria for privilege

- Privilege grants failed to meet requirements of policy
  - Rigid (e.g., view only, full rights) instead of flexible based upon the situation
  - Subjective (who you knew) instead of objective
  - Too long (userids grew stale) instead of tracking the work/credentials of the individual
  - Too broad (a whole data repository) rather than to specific data records or elements

Present

- Increased evaluation/use of tools to include more policy compliance *inside* enterprise systems
  - Rules engines
  - Role identification

- Incremental improvement, but still fail to be fully policy compliant
  - Collection of rules from business users tend to be anecdotal, incomplete, and/or incorrect
  - User authoring tools tend to lack necessary complexity or nuance
  - Role identification is one of several pieces needed to fufill requirements of policy

Goal

- Dynamic policy compliance
  - Allowing only those privileges
    - which are permitted by the *actual* rules as they apply to
      - the actor *at that moment*
      - the data *in context*
      - the specific environment
  - Requires turning policy into code

The Problem: Hypothetical

- Typical User Rule Statement:

  "Nurses may look at patient files."

- Typical Policy Statement:

  "Nurses, who are licensed in the state where they are working, have successfully completed HIPAA training in the last year, and are employees of the facility or employees of contractors currently providing services to the facility, may look at the files of patients on the floor or wing to which they are assigned, during the shift in which they are assigned to that floor or wing as well as one hour before and after that shift."

Shorter Rules aren't Real

- Multiple causes
  - Easier for business user to remember and say
    - Typically the result of passing original statement of policy from management or attorney through multiple hands over time
  - Easier for programmer to code
    - Nuances are often dropped from rule because they are believed to be of no value or subsumed by some other value
  - Easier to find/reach relevant data
    - Only requires access to two pieces of data/metadata – user role, data category of file

Real Rules are Hard

- Harder because:
  - Derived from multiple rules
    - One requires licensure, one is a federal privacy law, one requires hospital affiliation, one sets access policy
  - Data needed for compliance is in more places
    - Not all within the control of the party granting access
  - More complex
    - More conditions
    - Temporal requirements

Real Example

> “...No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—
>
> ...
>
> to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;”

Privacy Act, 5 USC § 552a(b) & (b)(7)

Real Example Challenges

- In this one portion of the Privacy Act:
  - 4 terms have specific, non-universal definitions
    - Stated elsewhere
  - 3 conditions
  - 3 exceptions
    - 3rd exception has 4 conditions
  - 4 parties are identified
  - 2 precursors are identified
  - 2 authorized purposes are identified

- The Privacy Act has 135 sub-rules

Improving Policy Expression

- Intermediate Isomorphic Representation
  - Intermediate
    - A form through which lawyers, policy makers, business users, and programmers can ensure they understand each other
  - Isomorphic:
    - A one for one representation
      - Avoids interpretations accidentally influencing outcomes
      - Easier to incorporate policy updates
      - Easier to incorporate administrative/procedural details
      - see, e.g., Bench-Capon, TJM & Coenen, FP, *Isomorphism and Legal Knowledge Based Systems*, Artificial Intelligence and Law, Vol 1, No 1, pp65-86 (1992).
  - A “Rosetta Stone”

Why “intermediate” representation?

- Don’t speak the same language
  - Lawyers
    - Write concept-based, run-on text
    - Read left to right
  - Computer Scientists
    - Write short, logic-based expressions
    - Read top to bottom
- Need a form both groups can readily assimilate

Why "isomorphic" representation?

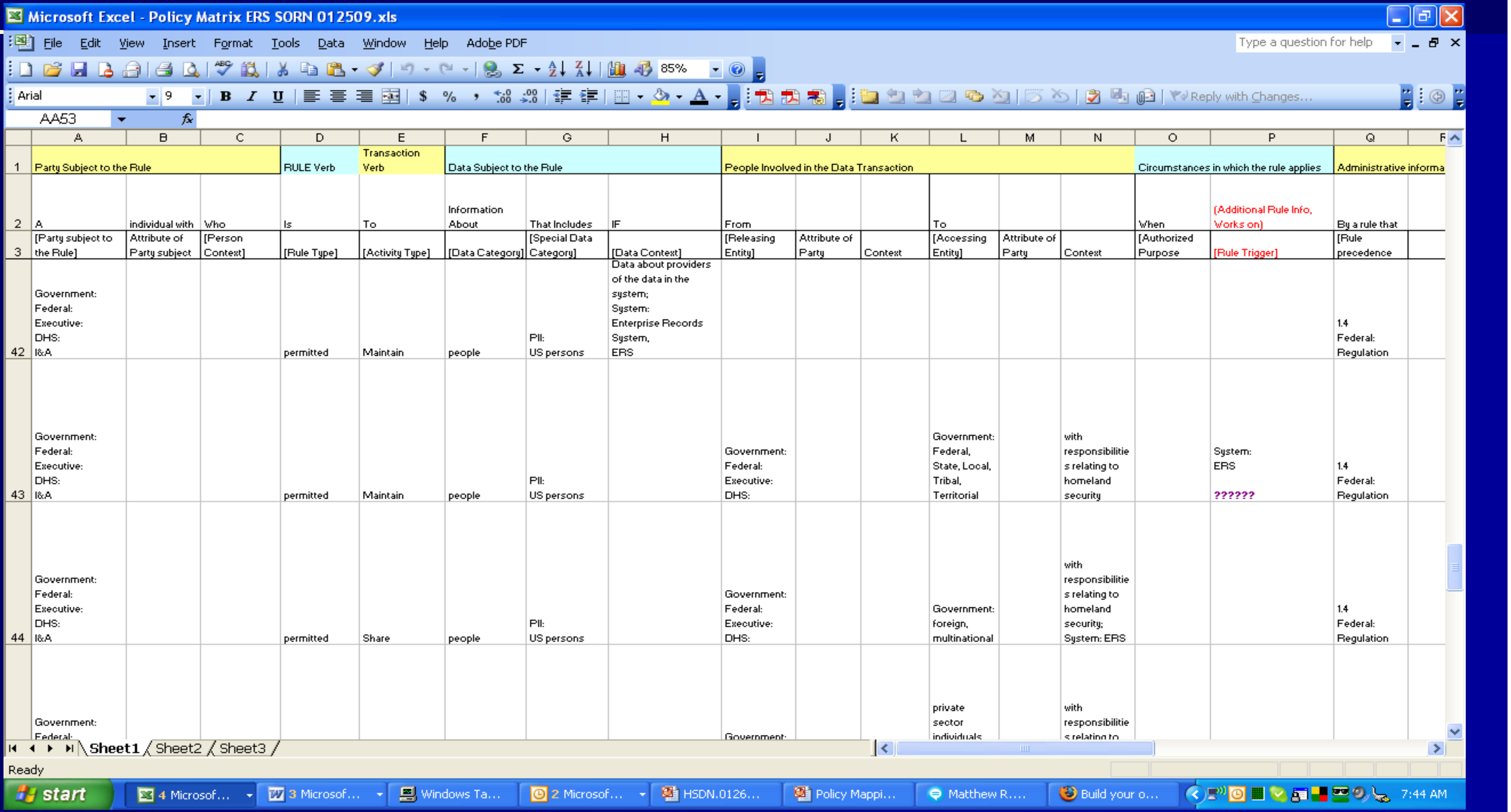
- Compound information differently
  - Lawyers
    - Add conditions, exceptions, and other compounding features
  - Computer Scientists
    - Compute the statements and represent the leanest form

- Using a consistent structure is needed for lawyers to validate the expressions

Example

- Policy Mapping Project (FY09)
  - Funded by DHS
  - Joint project of LawTechIntersect, LLC & PKH Enterprises, LLC
  - Will be presented in Track 4 Workshop

Policy Map: Rules (left)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Party Subject to the Rule			RULE Verb	Transaction Verb	Data Subject to the Rule			People Involved in the Data Transaction						Circumstances in which the rule applies		Administrative informa
2	A	individual with	Who	Is	To	Information About	That Includes	IF	From			To			When	(Additional Rule Info, Works on)	By a rule that
3	[Party subject to the Rule]	Attribute of Party subject	[Person Context]	[Rule Type]	[Activity Type]	[Data Category]	[Special Data Category]	[Data Context]	[Releasing Entity]	Attribute of Party	Context	[Accessing Entity]	Attribute of Party	Context	[Authorized Purpose	[Rule Trigger]	[Rule precedence
42	Government: Federal: Executive: DHS: I&A			permitted	Maintain	people	PII: US persons	Data about providers of the data in the system; System: Enterprise Records System, ERS									1.4 Federal: Regulation
43	Government: Federal: Executive: DHS: I&A			permitted	Maintain	people	PII: US persons		Government: Federal: Executive: DHS:			Government: Federal, State, Local, Tribal, Territorial		with responsibilitie s relating to homeland security		System: ERS ??????	1.4 Federal: Regulation
44	Government: Federal: Executive: DHS: I&A			permitted	Share	people	PII: US persons		Government: Federal: Executive: DHS:			Government: foreign, multinational		with responsibilitie s relating to homeland security; System: ERS			1.4 Federal: Regulation
	Government: Federal:								Government:			private sector individuals		with responsibilitie s relating to			

kkw@LawTechIntersect.com

Reading the Policy Map

Read across the spreadsheet, taking the column name and then a column value. (Blanks = “any”)

Rule Example:

A Government:Federal:Executive:DHS:I&A individual

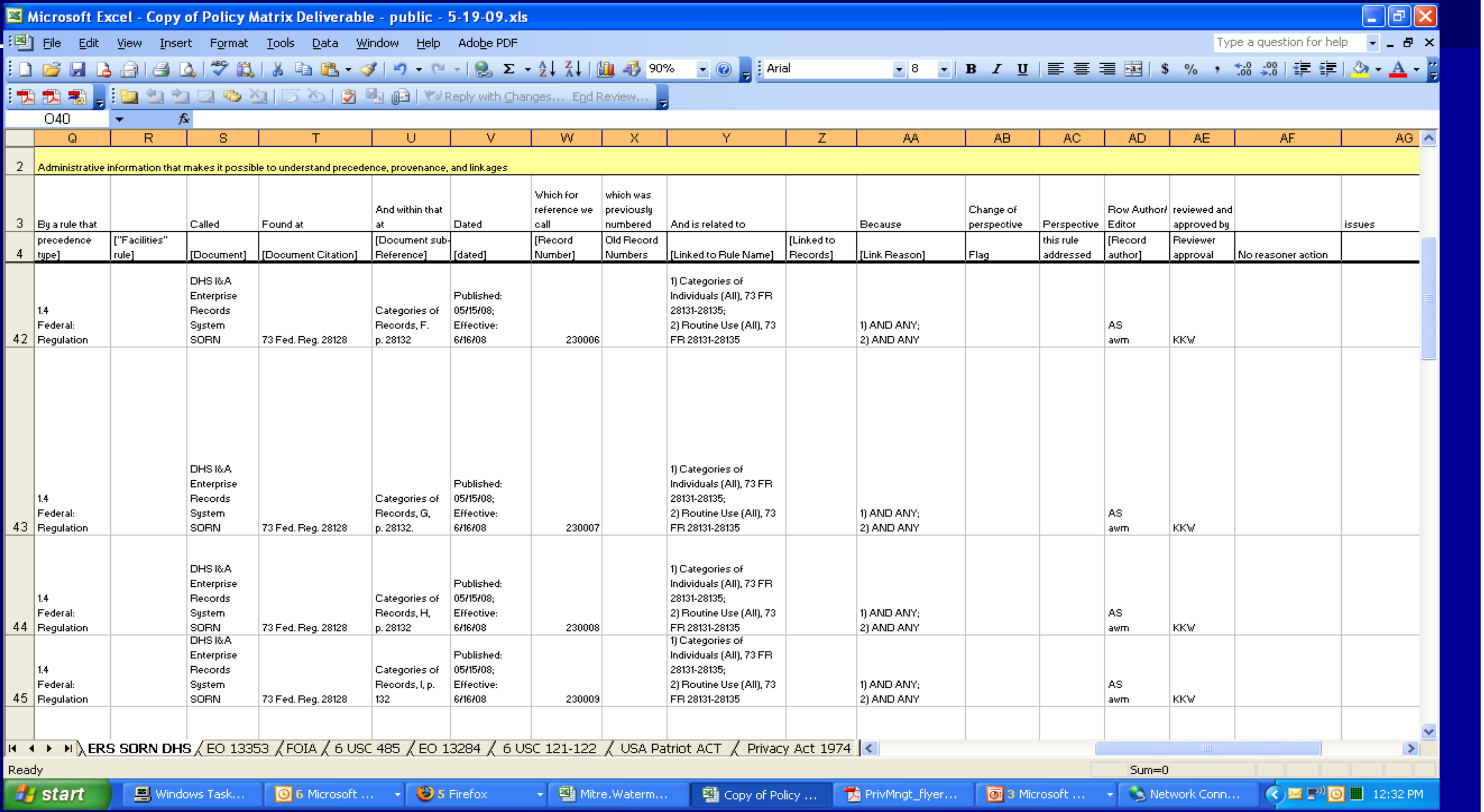
is permitted to retain

information about people including PII:US persons

if [the data is] about the providers of data

AND system:Enterprise Records System

Policy Map: Admin (right)



Microsoft Excel - Copy of Policy Matrix Deliverable - public - 5-19-09.xls

	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
2	Administrative information that makes it possible to understand precedence, provenance, and linkages																
3	By a rule that		Called	Found at	And within that at	Dated	Which for reference we call	which was previously numbered	And is related to		Because	Change of perspective	Perspective	Row Author/ Editor	reviewed and approved by		issues
4	precedence type]	["Facilities" rule]	[Document]	[Document Citation]	[Document sub-Reference]	[dated]	[Record Number]	Old Record Numbers	[Linked to Rule Name]	[Linked to Records]	[Link Reason]	Flag	this rule addressed	[Record author]	Reviewer approval	No reasoner action	
42	1.4 Federal: Regulation		DHS I&A Enterprise Records System SORN	73 Fed. Reg. 28128	Categories of Records, F. p. 28132	Published: 05/15/08; Effective: 6/16/08	230006		1) Categories of Individuals (All), 73 FR 28131-28135; 2) Routine Use (All), 73 FR 28131-28135		1) AND ANY; 2) AND ANY			AS awm	KKW		
43	1.4 Federal: Regulation		DHS I&A Enterprise Records System SORN	73 Fed. Reg. 28128	Categories of Records, G, p. 28132.	Published: 05/15/08; Effective: 6/16/08	230007		1) Categories of Individuals (All), 73 FR 28131-28135; 2) Routine Use (All), 73 FR 28131-28135		1) AND ANY; 2) AND ANY			AS awm	KKW		
44	1.4 Federal: Regulation		DHS I&A Enterprise Records System SORN	73 Fed. Reg. 28128	Categories of Records, H, p. 28132	Published: 05/15/08; Effective: 6/16/08	230008		1) Categories of Individuals (All), 73 FR 28131-28135; 2) Routine Use (All), 73 FR 28131-28135		1) AND ANY; 2) AND ANY			AS awm	KKW		
45	1.4 Federal: Regulation		DHS I&A Enterprise Records System SORN	73 Fed. Reg. 28128	Categories of Records, I, p. 132	Published: 05/15/08; Effective: 6/16/08	230009		1) Categories of Individuals (All), 73 FR 28131-28135; 2) Routine Use (All), 73 FR 28131-28135		1) AND ANY; 2) AND ANY			AS awm	KKW		

Reading the Policy Map

Read across the spreadsheet, taking the column name and then a column value. (Blanks = “any”)

Administrative Example:

If there’s a conflict, this rule is precedence level
1.4:Federal:Regulation.
[The rule is] called DHS ERS SORN,
found at 73 FR 28128,
And within that at Categories of Individuals, I, p. 28133,
Dated published: 05/15/08, effective 06/16/08
Which for reference we call [record number] 230009
And is linked to [record numbers] 23010, 23045, 23049]
Because [link is] AND

Benefits

- Accelerates enhancements to policy compliance technology
  - Showing policy language authors where enhanced expressivity is needed
  - Showing the ontologic and taxonomic categories in which things belong
  - Showing reasoner developers the level and type of complexity to be addressed

Benefits

- Revealing the variables and values that compliance systems need to reach
  - Allowing systems developers to determine the incremental order of implementation based upon
    - which are already available,
    - which must be captured in next system versions, and
    - which are too difficult and should be captured through user assertions