

IBM TJ Watson Research Center

Making Privacy Possible: Research on Organizational Privacy Technology

Clare-Marie Karat, Carolyn Brodie, and John Karat ckarat,brodiec,jkarat@us.ibm.com Privacy Enabling Technology Research Security, Networking and Privacy (SNAP)

IBM Research

11/11/2004

© 2004 IBM Corporation



Privacy Research Statement

- Most organizations store personal information (PI) data in heterogeneous server system environments.
- Currently they do not have a unified way of defining or implementing a privacy policy that encompasses both web and legacy applications across the different server platforms.
- This makes the management of PI data difficult for both enterprises and end users.



Progress to Date

- Identified Organizational Needs Initial survey (51 participants) asking about "top privacy concerns and technology needs"
- Established Scenarios In-Depth follow up (13 participants) to identify data flow and architectural concepts for privacy technology (e.g., sticky policy)
- Iterated on Designs Scenario-based walkthrough sessions of the privacy management prototype (SPARCLE) with target users (2 design iterations, 22 participants)
- Conducted Evaluations Laboratory study examining methods for policy authoring (36 participants)
- Developed Architecture Ongoing technical feasibility analysis



Identify Organizational Needs

- Recruited 51 Participants from Industry and Government:
 - –North America
 - -Europe
 - -Asia Pacific
- Sent Participants Privacy Questionnaires by E-Mail
- Asked about Top Concerns, Desired Function, Current Activities
- Analyzed Data by Industry (N=23) and Government (N=28)
- Questionnaire Response Rate was Approximately 80% from Customers



Top Privacy Concerns Expressed



- Industry and government patterns of concerns similar
- Industry more concerned about economic harm to brand
- Government more concerned about privacy violations by users outside the organization



Desired Privacy Functions



- Similar pattern across industry and government
- Desired policy/data portability
- Looked for easy to use authoring environment
- Wanted one solution for all organizational data



Iterative Design of Privacy Enabling Technology

- Focused on key privacy steps from previous analysis
- Established interaction requirements and a customervalidated design of a highly usable and effective privacy management tool called SPARCLE (Server Privacy ARchitecture and CapabiLity Enablement). Scope:
 - Author policies
 - Connect policy definition to system entities (Implement)
 - Check policy compliance (Audit)
- Iteratively designed and reviewed with customers
- 10 sessions with 22 target users over 2 design iterations

IBM TJ Watson Research Center

				_		
	-			1 2		
	-				-7	-
1		_	-			

	_12	at the second se
Elle Edit Yew Favorites Iools Help		
+ Bask + + - O (1) (2) (2) Search (1) Favorites (3) Media (3) (2) - (3) (2) - (3)		
Links Customize Links CiPree Hotmail CIBM Business Transformation Homepage CIBM Business Transformation CIBM (Home Page	Policy
Agistress III Re:///C:/Documents9620and9620Settings/brodec/My9620Documents/PrivacyPrototype/PolicyCreation/policyCreation	122.htm?group=Custo 🛀 🧬G	Anthonion
Author Transform Map User Map Data Map Map Map Verify Policy Policy Categories Categories Purpose/Actions Conditions Obligations Policy	-	And
Policy Name: Policy DrugsAreUs Privacy FPolicy Date: 3/1/04 Source File: Privacy1.txt Load	£	Implementation
Description: This policy defines the uses of customer personal information.		Task Steps
Current Step: Author Policy	Same	- and steps
Choose a policy template and modify the privacy rules provided as needed or type your policy rules below using the example and information on the <u>Help</u> page as needed.		Privacy Policy
Privacy Policy None Selected		Template
Termi ates: Parent Company Privacy Policy for US (HIPAA)		
Parent Company Privacy Policy for Canada		Selection List
Parent Company Privacy Policy for Canada Example Rule Guide:		Selection List Privacy
[Example Rule Guide: [User Category(les)] can [Action(s)] [Data Category(les)] for the purpose(s) of [Purpose(s)] if.		Privacy Policy Rule
[Verent Company Privacy Policy for Canada Example Rule Guide: [User Category(les)] can [Action(s)] [Data Category(les)] for the purpose(s) of [Purpose(s)] if [(optional) Condition(s)] with [(optional) Obligation(s)]. 1. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and date of birth to help confirm identity.		Selection List Privacy Policy Rule Guide
[User Category(les)] can [Action(s)] [Data Category(les)] for the purpose(s) of [Purpose(s)] if. [(optional) Condition(s)] with [(optional) Obligation(s)]. 1. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and date of birth to help confirm identity. 2. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and e-mail addresses to respond to inquiries and to notify customers about issues regarding orders.	1	Selection List Privacy Policy Rule Guide Free Form
Parent Company Privacy Policy for Canada Example Rule Guide: [User Category(les)] can [Action(s)] [Data Category(les)] for the purpose(s) of [Purpose(s)] if. [(optional) Condition(s)] with [(optional) Obligation(s)]. 1. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and date of birth to help confirm identity. 2. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and e-mail addresses to respond to inquiries and to notify customers about issues regarding orders. 3. Shipping Reps can use customer name and customer mailing addresses to ship orders.		Selection List Privacy Policy Rule Guide Free Form Area for Typing
Parent Company Privacy Policy for Canada Example Rule Guide: [User Category(les)] can [Action(s)] [Data Category(les)] for the purpose(s) of [Purpose(s)] if. [optional) Condition(s)] with [(optional) Obligation(s)]. 1. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and date of birth to help confirm identity. 2. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and e-mail addresses to respond to inquiries and to notify customers about issues regarding orders. 3. Shipping Reps can use customer name and customer mailing addresses to ship orders. 4. Billing Reps can use credit catd numbers for order processing.		Selection List Privacy Policy Rule Guide Free Form Area for Typing Natural
Parent Company Privacy Policy for Canada Example Rule Guide: [User Category(les)] can [Action(s)] [Data Category(les)] for the purpose(s) of [Purpose(s)] if [optional) Condition(s)] with [(optional) Obligation(s)]. 1. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and date of birth to help confirm identity. 2. Customer Service Reps, Pharmacists, and Billing Reps can collect and use customer name and e-mail addresses to respond to inquiries and to notify customers about issues regarding orders. 3. Shipping Reps can use customer name and customer mailing addresses to ship orders. 4. Billing Reps can use credit card numbers for order processing, if the customer is notified by email of the change.		Selection List Privacy Policy Rule Guide Free Form Area for Typing Natural Language

IBM TJ Watson Research Center

		-	_	
_	-	-		
	_			
		_	_	_

🕙 Rules Creation#&#&</th><th>#&#&#&#&#& - Microsoft In</th><th>nternet Explorer</th><th></th><th></th><th>_ 🗆 🛛</th></tr><tr><th>Ele Edit View Favo</th><th>orites Iools Help</th><th></th><th></th><th></th><th>27</th></tr><tr><th>G Back + O +</th><th>🖹 📓 🏠 🔎 Search</th><th>📌 Favorites 🜒 Media 🌾</th><th>3 🔗 🖉 🗖 · 🗖</th><th>8</th><th></th></tr><tr><td>Einks 🙆 Search the Web</td><td>with Lycos</td><td>* Address file:///C:/Do</td><td>ocuments%20and%20Settings/Ad</td><td>ministrator/My%20Documents/Priva</td><td>acyPrototype/rules/rule: 🗙 🄁 Go</td></tr><tr><td>Privacy Policy Temple</td><td>ites:</td><td>Parent Company Privacy P Parent Company Privacy P</td><td>Policy for US (HIPAA) Policy for Canada</td><td></td><td>^</td></tr><tr><td>Parsed Rule:</td><td>1. Customer Service Reps, and Billi</td><td>ng Reps can Collect, or Use Custor</td><td>ner Name, and Date Of Birth for the</td><td>purpose(s) of Confirm Identity</td><td>*</td></tr><tr><td>Original Rules:</td><td> Customer Service Reps, I help confirm identity. </td><td>Pharmacists, and Billing Rep</td><td>s can collect and use custor</td><td>mer name and date of birth to</td><td>Parsed Rule</td></tr><tr><td>Add Rule</td><td>obligations</td><td>ose the appropriate user ca</td><td>tegones, data categones, pi</td><td>urposes, actions, conditions,</td><td>and Original Rule</td></tr><tr><td>Modify Rule Delete Rule</td><td>To modify a privacy rule, ch obligations. Click button to delete the ch</td><td>oose the appropriate user co osen rule.</td><td>ategories, data categories, p</td><td>purpose, actions, conditions,</td><td>and Rule Elements</td></tr><tr><th>User Categories</th><th>Actions</th><th>Data Categories</th><th>Purposes</th><th>Conditions</th><th>Obligations</th></tr><tr><th colspan=2>None Selected None Selected Customer Service Reps Collect Use Billing Reps Modify Shipping Reps</th><th>None Selected Customer Name Date Of Birth e Mail Customer Mailing Address</th><th>None Selected Confirm Identity Respond to Inquiry Notification Send Marketing Information</th><th>None Selected customer has opted-in</th><th>None Selected Notification</th></tr><tr><th>Marketing Reps</th><th></th><th>Credit Card Number</th><th>Ship Order Order Processing</th><th></th><th></th></tr><tr><th>Add Delete</th><th>Add Delete</th><th>Add Delete</th><th>Add Delete</th><th>Add Delete</th><th>Add Delete</th></tr><tr><td>a</td><td></td><td></td><td></td><td></td><td>🚽 My Computer</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>oarch</td><td></td><td>11/1-</td><td>1/2004</td><td>© 2004 IPM Corrected</td></tr></tbody></table>
--

_		_		_	
_	_	-	-	_	-
_	_	-	-	-	-





Next Steps

- Continue enrichment and testing of the prototype with target customers!
- Exploring relationship to compliance issues