

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

10/14/2004

© 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

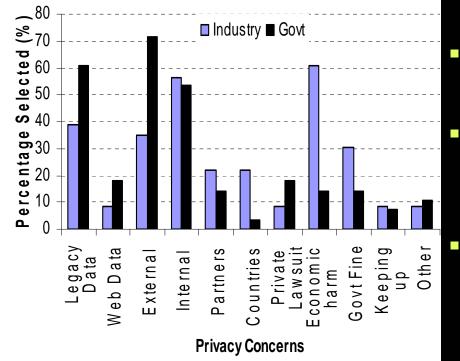


Identify Organizational Needs

- 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



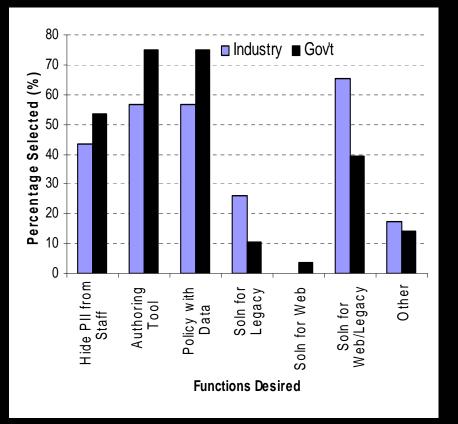
Top Privacy Concerns Expressed



- 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
- I0 sessions with 22 target users over 2 design iterations

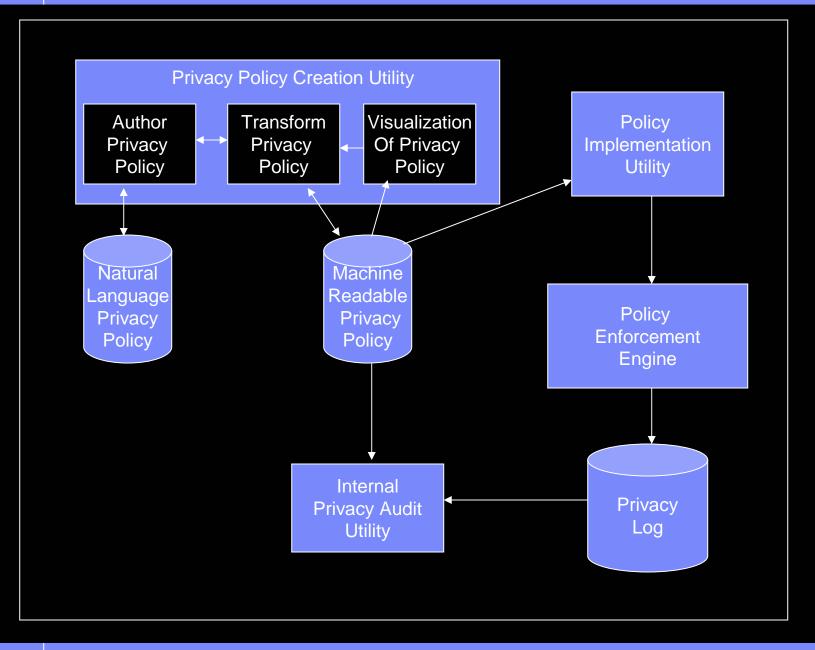
_	 _
	1.1.1
_	

❑ Author Policy#&#&#&#&#&#&#& - Nicrosoft Internet Explorer</th><th></th><th></th></tr><tr><th>Elle Edit View Favorites Icols Help</th><th>18</th><th></th></tr><tr><th>+Set + → + @ 3 2 @Search BFavorites @Media 3 5+ 3 2 + 3</th><th></th><th>10000 10(00)</th></tr><tr><th>Unks Customize Links CiFree Hotmal CIBM Business Transformation Homepage CIBM Business Transformation</th><th>the Area in the second s</th><th>Policy</th></tr><tr><th>Address E Tie:///C:/Documents%20and%20Settings/brodiec/My%20Documents/PrivacyPrototype/PolicyCreation/policyCreat</th><th></th><th>The second s</th></tr><tr><th>Author Transform Map User Map Data Map Map Map Verify Policy Policy Categories Categories Purpose/Actions Conditions Obligations Policy</th><th></th><th>Authoring</th></tr><tr><td>Policy Drame Arable Privary EPolicy Date: 2/1.04 Source File: Privary1 bt</td><td></td><td>And</td></tr><tr><td>Name:</td><td><u></u></td><td>Implementation</td></tr><tr><td>Policy Description: This policy defines the uses of customer personal information.</td><td></td><td>Task Steps</td></tr><tr><th>Current Step: Author Policy</th><th>Save</th><th>Tusk Steps</th></tr><tr><th>Choose a policy template and modify the privacy rules provided as needed or type your policy rule</th><th>A CONTRACT OF A CONTRACT OF A</th><th></th></tr><tr><th>below using the example and information on the Help page as needed.</th><th></th><th>Privacy</th></tr><tr><th></th><th></th><th>Policy</th></tr><tr><th>Alexandra Constant</th><th></th><th>Template</th></tr><tr><th>Privacy Policy None Selected Parent Company Privacy Policy for US (HIPAA)</th><th></th><th>- 24 - 26 - 26 - 27 - 27 - 27 - 27 - 27 - 27</th></tr><tr><td>Templates: Parent Company Privacy Policy for Canada</td><td></td><td>Selection List</td></tr><tr><th></th><th></th><th></th></tr><tr><td>Example Rule Guide:</td><td>7</td><td></td></tr><tr><th></th><th></th><th>Privacy</th></tr><tr><th>[User Category(ies)] can [Action(s)] [Data Category(ies)] for the purpose(s) of [Purpose(s)] if [(optional) Condition(s)] with [(optional) Obligation(s)].</th><th></th><th>Policy Rule</th></tr><tr><td>1. Customer Service Reps, Pharmacists, and Billing Reps can collect and use</td><td>3</td><td>12 22</td></tr><tr><td>customer name and date of birth to help confirm identity.</td><td></td><td>Guide</td></tr><tr><td>2. Customer Service Reps, Pharmacists, and Billing Reps can collect and use</td><td></td><td>1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -</td></tr><tr><td>customet name and e-mail addresses to respond to inquiries and to notify customers about issues regarding orders.</td><td></td><td>Free Form</td></tr><tr><th></th><th></th><th>Area for</th></tr><tr><td> Shipping Reps can use customer name and customer mailing addresses to ship lorders. </td><td></td><td>방법(학생은 것은 학생님).</td></tr><tr><td></td><td></td><td>Typing</td></tr><tr><td>4. Billing Reps can use credit card numbers for order processing.</td><td></td><td>Natural</td></tr><tr><td>5. Customer Service Reps can modify credit card numbers for order processing, if the customer is notified by email of the change.</td><td></td><td>Language</td></tr><tr><td>The one entropy as mercane all many or one country.</td><td></td><td>00-</td></tr><tr><td></td><td>MI My Computer</td><td>Privacy Policy</td></tr></tbody></table>

_	_	
	_	
_	_	= 7 =

Rules Creation#&#&#&#&#&#&#& - Microsoft In</th><th>ternet Explorer</th><th></th><th></th><th></th></tr><tr><th>Eile Edit View Favorites Tools Help</th><th></th><th></th><th></th><th><u>Av</u></th></tr><tr><th>🕜 Back - 🕥 - 💌 🗟 🚮 🔎 Search</th><th>🔆 Favorites Media 🤞</th><th>8 🔗 - 🍯 🖬 - 🚺</th><th>3</th><th></th></tr><tr><th>Links 👹 Search the Web with Lycos</th><th>* Address file:///C:/Do</th><th>ocuments%20and%20Settings/Adr</th><th>ninistrator/My%20Documents/Priva</th><th>cyPrototype/rules/rule: 📉 🛃 Go</th></tr><tr><th>Privacy Policy Templates:</th><th>Parent Company Privacy F Parent Company Privacy F</th><th></th><th></th><th></th></tr><tr><th>Parsed Rule: 1. Customer Service Reps, and Billin 1. Customer Service Reps, P Original Rules: help confirm identity.</th><th></th><th></th><th></th><th>Parsed Rule</th></tr><tr><th>Add Rule To define a privacy rule, choor obligations. Modify Rule To modify a privacy rule, choor obligations. Delete Rule Click button to delete the choor obligations.</th><th>oose the appropriate user c</th><th></th><th></th><th></th></tr><tr><th>User Categories Actions</th><th>Data Categories</th><th>Purposes</th><th>Conditions</th><th>Obligations</th></tr><tr><th>None Selected Collect Customer Service Reps Collect Pharmacists Use Billing Reps Modify Shipping Reps Marketing Reps</th><th>None Selected Customer Name Date Of Birth eMail Customer Mailing Address Credit Card Number</th><th>None Selected Confirm Identity Respond to Inquiry Notification Send Marketing Information Ship Order Order Processing</th><th>None Selected customer has opted in</th><th>None Selected Notification</th></tr><tr><th>Add Delete Add Delete</th><th>Add Delete</th><th>Add Delete</th><th>Add Delete</th><th>Add Delete</th></tr><tr><th>8</th><th></th><th></th><th></th><th>S My Computer</th></tr><tr><th></th><th></th><th></th><th></th><th></th></tr></tbody></table>
--

_	_	





Next Steps

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