Personalized Privacy Policies: Challenges for Data Loss Prevention

Nathan Gnanasambandam
nathan.gnanasambandam@xerox.com

Jessica Staddon
staddon@parc.com

Abstract

Given the prevalence of data leaks, organizations appreciate the importance of implementing privacy policies to protect sensitive data. The growing field of Data Loss Prevention (DLP) offers tools to enforce such policies for both data stored within an organization and data being shared outside of an organization (e.g. through email). While the DLP community has given much attention to the problem of enforcing data privacy policies in a comprehensive manner, little has been done to support the development of such policies. We present a small user study demonstrating that developing such policies is also a very challenging problem. In our study, users were asked to evaluate various expressive file names for sensitivity; that is, they were asked to consider how broadly they were willing to share those filenames both inside and outside their place of employment. The study indicates that users interpret their employer’s privacy concerns in differing ways, resulting in complex, personalized privacy policies at the user end. These results suggest that it may be difficult for users to form a coherent organization-level privacy policy and that the results of a DLP-based enforcement of such policies (e.g. quarantined emails) may be confusing for many users in the organization.

1. Introduction

A core tool in effective enterprise privacy is a privacy policy. The privacy policy determines what information is sensitive and should not leave the organization without appropriate approvals, and what information is nonsensitive, and thus free to be disseminated. The privacy policy is implemented within what the data loss prevention (DLP) market, often calls a “content monitor”. The content monitor checks any content leaving the enterprise against the privacy policy, with the goal of ensuring that no sensitive information (e.g. customer information, intellectual property, etc.) leaves the enterprise inappropriately.

Writing the enterprise’s privacy policy is a very challenging task as it requires a broad knowledge of the enterprise’s data and business. In addition, the members of the organization who have the necessary broad knowledge are often unfamiliar with the technical side of specifying and implementing policies. To remedy this, there is a growing interest in developing tools supporting the natural language expression of policies, and the automatic implementation of such policies. While we believe these tools are very useful and are going in the right direction, we raise as an issue the importance of developing tools for interpreting the policy expressions given by users and understanding how to detect and address biases, misunderstandings and trust judgements that color their privacy specifications.

Our paper is motivated by a small study in which user print job data was collected for several months, and users were questioned about the sensitivity of their data. Our study consisted of 10 users and their data consists of the filename of each print job, the time of the print job and the size of the job. With the popularity of expressive filenames, we found that most of the files printed during the study were classifiable by topic simply given their name (e.g. “revolutionary_war_cereal_box_stuff_2.doc”, “http://www.apexdevnet.com/media/06.2328”, “2009 RNA dinner program.doc”). Subsequent to data gathering the users were questioned about whom they would be willing to share the print job information with and how related it was to their work.

We found a remarkable variety in privacy preferences amongst the users. The users varied greatly in how much information they were willing to share with colleagues, management and friends. In addition, for most users there appeared to be high-level, strongly implemented rules, governing their sharing decisions. Yes, those rules varied a lot by user. In addition, even on files that were printed by more than one user, there was frequent disagreement about how the files could be shared and with whom.

While our study was a small one, we believe that the results indicate that the issue of personalization of privacy policies warrants more attention as it may have strong impact on an organization’s ability to specify an accurate privacy policy.

2. Related Work

The focus of our study is content-driven privacy policies for enterprise data. Our work is most closely related to the efforts at natural language support for security policy authoring (e.g. (Vaniea et al. 2008; Reeder et al. 2008; Bauer et al. 2008; Reeder et al. 2007)). However, we differ from these works in that they generally focus on the broader problem of access control and assume some categorization of the data is in place. In contrast, we are focusing on pri-
Table 1: The job statistics for the 10 participants in the user study. Job data was collected over a period of 5 months; roughly 4 months in 2008 and 1 month in 2009.

<table>
<thead>
<tr>
<th>User</th>
<th>Total Number of Jobs</th>
<th>Number of Jobs Evaluated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>103</td>
<td>57</td>
</tr>
<tr>
<td>2</td>
<td>126</td>
<td>59</td>
</tr>
<tr>
<td>3</td>
<td>134</td>
<td>58</td>
</tr>
<tr>
<td>4</td>
<td>125</td>
<td>62</td>
</tr>
<tr>
<td>5</td>
<td>126</td>
<td>58</td>
</tr>
<tr>
<td>6</td>
<td>47</td>
<td>34</td>
</tr>
<tr>
<td>7</td>
<td>287</td>
<td>67</td>
</tr>
<tr>
<td>8</td>
<td>59</td>
<td>23</td>
</tr>
<tr>
<td>9</td>
<td>104</td>
<td>52</td>
</tr>
<tr>
<td>10</td>
<td>33</td>
<td>20</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>1144</strong></td>
<td><strong>490</strong></td>
</tr>
</tbody>
</table>

Privacy issues within the enterprise in the context of unstructured data.

Finally, we note that our results are further evidence of the challenges of reconciling security/privacy and usability (see, for example, (Adams and Sasse 1999b; 1999a)) and echo results in the access control world attesting to the complexity of access rights desired by users (Smetters and Good 2009; Ahern et al. 2007).

3. Study

We collected job data from 2 printers within Xerox corporation for a period of roughly 5 months each. For each printer we collected the job size, the number of pages in the job, the date and duration of the job, the name of the user who sent the job, and the job name (including the filename). For the purposes of this paper we rely exclusively on the filenames and the associated user names.

We summarize the print job data for the 10 users who participated in our study in Table 1 along with the percentage of flagged jobs for each of algorithms outlined below.

To evaluate the accuracy of our results we conducted a small study in which 10 users were asked to evaluate MFD jobs randomly selected from the jobs they had to one of the 2 MFDs during the 5 month period. To minimize the burden on users, they were asked about a proper subset of their jobs. The number of jobs evaluated by each user is in Table 1.

The users were asked the following questions about each job:

1. Are you willing to share this job information and the fact that you sent this job to the enterprise MFD\(^1\) with:
   (a) Colleagues? (Y/N)
   (b) Company management? (Y/N)

2. Would you use this job information to conduct a search on:
   (a) A Web search engine (e.g. Google)? (Y/N)
   (b) An online library (e.g. IEEE Online)? (Y/N)

3. How closely is this job related to your work on a scale of 1-5 (5=most relevant)?

In the survey, the users were asked to evaluate a total of 490 jobs. Out of these jobs, 478 jobs were unique; a maximum of 12 jobs were dispatched to the printers more than once.

A total of ten participants were involved in the study. Out of these ten, five are Xerox researchers, two are research managers, two are software developers and one is an administrator. Each of the users that signed up for the study were individually instructed about how to answer the aforementioned questions. Also, an email was sent with an example. Both in the email and in a face-to-face meeting prior to the survey, the example discussed was a job that contained the title of a study in a popular research area in distributed systems (i.e. “grid_2009_autonomic_virtualization_modeling.pdf”).

It was provided as an example of a print job that did not present a privacy risk because the file name does not reveal any sensitive information. All ten survey takers agreed that the aforementioned example was indeed not a privacy risk. Furthermore, the study participants were told that for all jobs in the survey, only superficial job information such as titles and time-stamps were used to determine sensitivity, not the file content.

4. Results

To analyze the survey results we calculated the strength of all association rules (e.g.,(Hipp, Gntzer, and Nakhaiezadeh 2000; Agrawal, Imielinski, and Swami 1993)) between all possible answers to the 6 questions in the survey. That is, if question \(Q_j\) supports the answer \(A_i\) (i.e., \(A_i\) would be either “yes” or “no” in the case of questions 1-2, and a positive integer of size at most 5, in the case of the last question) and question \(Q_j\) supports the answer \(A_j\), then we calculated the probability, \(P(Q_j = A_j \mid Q_i = A_i)\), as a measure of the confidence of the rule, \((Q_i = A_i) \rightarrow (Q_j = A_j)\). Hence, we considered \((\frac{5}{2}) \cdot 2 \cdot 4 + 5 \cdot 2 \cdot 5 = 180\) association rules.

We focused on rules that we term “strong”, by which we mean rules having a probability of at least .75 and a support (i.e. number of instances) of at least 10. While any such cut-off would be partly arbitrary, we chose these numbers based on our understanding of the data set. In particular, probabilities in the data set tend to cluster close to 0, to .5 or to be larger than .75. For support, there was the possibility of documents that blurred the line between work and non-work activities (e.g. directions to a restaurant near a work-related conference or an invitation to a work-sponsored social event to which family members are invited) that we felt a cut-off was prudent in order to not confuse the results. Note that users 8 and 10, who each evaluated only 23 and 20 jobs,
respectively, were less likely to have strong rules than the other study participants.

We summarize the strong rules found by user in Table 2. Note that with the exception of user 7, all the users printed at least as many non-work-related files as work-related files.

Overall, we found a high degree of rule disagreement amongst the participants. In particular, out of the 91 strong rules found, there were 23 pairs of “opposite” rules (i.e. 46 rules total), that is rule pairs of the form \((Q_i = A_i) \rightarrow (Q_j = “Yes”)\) and \((Q_i = A_i) \rightarrow (Q_j = “No”))\). In addition, almost 33% of the rules had support of 1, more than 73% of the rules had support of 3 or less, and only 15% of the rules had support at least 5. Of course, there may be many reasons for this disagreement, including the fact that users were generally dealing with different files and they may also have interpreted the survey directions differently. Nevertheless, the fact that users disagree substantially even on the 15 print jobs shared by more than 1 user (i.e. at least 2 people printed the same file) indicates the challenges inherent in establishing privacy policies that accurately reflect the privacy concerns of users. We discuss the results in more detail below, and suggest some avenues that may lead to more accurate access control within the enterprise.

**Areas of Agreement.** Most users in the study prefer to share less of their jobs with management than with colleagues. Indeed the rule, (Will not share with colleagues) \(\rightarrow\) (Will not share with management), is one of the most popular strong rules, with a support of 7 (i.e. the survey results of 7 users demonstrated this as a strong rule). In addition, the rule (Will not share with management) \(\rightarrow\) (Will share with colleagues), has positive probability for all but 3 users. Of the 3 remaining users, 2 draw no distinction between management and colleagues (they are either willing to share job info with both or neither) and the third is unwilling to share job information with management, colleagues, search engines or online libraries, with the exception of a single job that they are willing to share with all these entities.

The other main consistency across study participants is in a decrease in willingness to share with online libraries as opposed to search engines. For example, one of the most popular strong rules is: (Will not share with search engine) \(\rightarrow\) (Will not share with online libraries), whereas, \(P((Will\ share\ with\ search\ engine)\mid(Will\ not\ share\ with\ online\ libraries))\) is positive for 5 of the 10 users. This may reflect the broader use of search engines than online libraries (i.e. search is useful for more content than online libraries), however it may also reflect a difference in the trust users place in search engines and online libraries.

**Areas of Disagreement.** There are 15 unique documents that were printed and evaluated by at least 2 users. For 12 of those documents, the users disagreed on at least one of the “sharing” questions above (questions 1 and 2), and the average number of question disagreements was 2.4. The questions with the most disagreement were 1(c), “Are you willing to share this job information and the fact that you sent this job to the enterprise MFD with friends?”, and 2(a), “Would you use this job information to conduct a search on a Web search engine?”. The question with the least disagreement was “Are you willing to share this job information and the fact that you sent this job to the enterprise MFD with colleagues?”.

In addition, as briefly mentioned above, there are many conflicting strong rules that had near equal support. For example, while 4 users demonstrated (Will not share with online libraries) \(\rightarrow\) (Will not share with colleagues) as a strong rule, 3 demonstrated the opposite as a strong rule, that is: (Will not share with online libraries) \(\rightarrow\) (Will share with colleagues). Similarly, 4 users demonstrated that they would not share clearly non-work-related jobs (i.e. those with an answer of “1” to question 3) with colleagues, while 3 users demonstrated they would share those jobs with colleagues. As yet another example, 2 users demonstrated they would share jobs they share with friends with management as well, as a strong rule, while 3 users demonstrated the opposite as a strong rule: they would not share with management jobs they share with friends.

Finally, some study participants appeared to have difficulty distinguishing between personal privacy and enterprise privacy. In particular, 4 users demonstrated they would not share any print jobs that were clearly not work-related (i.e. the answer to question 3 was “1”) with search engines, yet they were likely to share work-related jobs (i.e. those with answer “5” to question 3) with search engines.

**Opportunities for Better Access Control.** With the increased interest in supporting the expression of privacy

---

Table 2: A listing of the number of strong rules and work/non-work related jobs for each user.

<table>
<thead>
<tr>
<th>User</th>
<th>Number of Strong Rules</th>
<th>Number of Work-related Jobs (5-6 on Question 3)</th>
<th>Number of Non-work-related Jobs (1-2 on Question 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30</td>
<td>14</td>
<td>38</td>
</tr>
<tr>
<td>2</td>
<td>28</td>
<td>6</td>
<td>51</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>24</td>
<td>4</td>
<td>42</td>
</tr>
<tr>
<td>5</td>
<td>33</td>
<td>9</td>
<td>46</td>
</tr>
<tr>
<td>6</td>
<td>22</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>7</td>
<td>28</td>
<td>28</td>
<td>27</td>
</tr>
<tr>
<td>8</td>
<td>25</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>24</td>
<td>13</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Totals</td>
<td>1144</td>
<td>117</td>
<td>293</td>
</tr>
</tbody>
</table>

---

Note that if this is the right interpretation it represents a misunderstanding of the survey on the part of the users, as the survey attempted to ask whether users would trust online libraries and search engines with their print jobs, not whether those services would be useful in connection with their print jobs.
policies in natural language, it seems reasonable to consider ways in which to query users to elicit accurate privacy preferences. Ideally, such questions would be generally applicable (i.e., not specific to an organization’s structure) and unlikely to make a user feel uncomfortable or steer them in the direction of a “right” answer. For example, a user who is asked, “Would you share this content with your boss?” might worry that answering “no” would suggest that they are spending time on things unrelated to work, or that they are not confident in their performance or communicating well with their boss, thus dissuading them from answering honestly. Our survey suggests that for some users, there may be more innocuous alternatives to questions like these, based on the user’s privacy policies. For example, 5 users demonstrated that if they would not share a job with an online library, then they also would not share that job with management. Similarly, 4 users demonstrated that if they would not share a job with an online library, then they also would not share it with colleagues. For such users, it may be possible to identify the right access controls for content by simply asking whether or not it should be shared with an online library, a far less “loaded” question than asking directly about sharing with management and/or colleagues.

The fundamental question that data loss prevention (DLP) seeks to address is whether or not it is acceptable to share certain content outside an organization. Our study indicates that this may be too coarse of a question, given the differences in opinion about sharing job information with search engines and online libraries (both external to the organization). More accurate DLP may be possible by identifying concrete examples of external sharing that better reflect the user’s privacy concerns about particular content.

5. Conclusion

Our small study indicates that user privacy concerns around enterprise documents are complex and varying. This may be the result of difficulty distinguishing personal privacy goals from those of the enterprise (or other confusion around the notion of enterprise privacy), or it may indicate fundamental differences in user views on enterprise privacy. The predominance of non-work-related files may add to privacy confusion. In either case, this complexity and variation warrants further study as it indicates there are substantial challenges to be overcome in crafting consistent, accurate and user-intelligible enterprise privacy policies. In addition, we emphasize that the question of how to elicit accurate privacy policies from users merits further attention.

References