Project Number: KXF-PRIV

HUMAN INTERPRETATION OF PRIVACY POLICY

An Interactive Qualifying Project Report:

submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

by

Steven Rose **Elijah Forbes-Summers**

Date: April 21, 2007

Approved:

Professor Kathi Fisler, Advisor

1. privacy
2. psychology
3. access-control policy

Abstract

Building privacy policies into software systems can greatly increase the ease of handling sensitive information and reduce the possibility of information misuse. However, such a system only works if the way the software enforces the policy matches user expectations about the policy. Therefore it is important that we understand how users think about privacy policies to help negotiate discrepancies between user and system interpretations of a policy.

Acknowledgements

We would like to thank our advisor, Professor Kathi Fisler, for her guidance and patience. We would also like to thank Professor George Heineman and Roger Donahue for their work on the Electronic Advising Folder system and for taking the time to talk with us about the system.

Contents

List of Figures

List of Tables

1. Introduction

The way that private information is recorded, stored, and accessed is changing. Increasingly, this information is being used electronically. Many benefits accompany this change; the speed and ease with which information can be stored and managed has greatly increased. However, the electronic use of sensitive information raises concerns due to the lack of human involvement during the operation of these electronic systems.

There is usually a policy in place that determines how sensitive information is protected. Traditionally it was the job of the people who managed the information to interpret the policy and make sure information was handled in accordance with it. If there was a need to access the information these people could determine if it was a reasonable need according to the policy.

A privacy policy exists when a computer is put in control of access to information as well, albeit specified differently. Although the computer is put in control of the information, the policy must still be written by humans. The important difference is that in this case the policy is interpreted precisely (a computer cannot get the “gist” of what a policy is describing). This means that the policy must be exact in its description of how information can be accessed. More importantly, if there is a error in the policy the computer won't have the common sense to do the right thing. Therefore it is important that the specification of the privacy policy accurately capture people's intent if we expect the computer to protect information appropriately.

There are typically many different factors that affect the content of the privacy policy. Legal requirements, institutional regulations, and user preferences all significantly contribute to the final policy (their importance in the final policy given from greatest to

least in order of listing). The sources that remain fairly static (legal and institutional requirements) are generally easy to describe within a privacy policy. The difficulty comes when we need to make changes to a policy. This comes up often in the case of describing user privacy preferences, especially if the users themselves are given control over this portion of the policy.

The problem with giving users control of parts of the policy is that their understanding of what a rule in the policy means might differ from the way the computer interprets that rule. There is also the problem of describing the policy to the user. The information the user provides and the way they use the system depends on their understanding of the privacy provided by the system.

This project is designed to explore how people articulate policy. People are generally more interested and hence provide better responses when the example chosen affects them. Luckily, a very useful example is available- the Electronic Advising Folder.

1.1 Electronic Advising Folder

As an example case we will be investigating the privacy considerations of the Electronic Advising Folder (EAF). The EAF is the end-result of a proposal to transition student advising records from their current paper form to an easier-to-use electronic system. Currently, advisors have access to some information about the student through web interfaces. Advisors are also required to maintain a paper advising folder for each advisee. However, there are complaints about the current system. The degree evaluations generated by the current web interface are sometimes misleading; also they are not appropriate for students pursuing programs more complicated than a single major (dual major, minors, etc.). There is no way for advisors to keep up to date on the progress of

their advisees other than by generating a degree evaluation for them (or generating one by hand). Maintaining the paper advising folder is a time-consuming process for advisors; the folders are also prone to being misplaced or out-of-date. There is no system for recording advisee-advisor communication. Students are provided little assistance for creating academic plans.

Due to these issues, the planned EAF system will provide an all-in-one interface for advising. Students will be able to view communication from advisors and academic advising offices along with information about their progress. Advisors will be able to sort their list of advisees in various ways and can be made aware of any potential problems with their students. Tools will be provided to help students prepare academic plans and to have those plans automatically evaluated to make sure they address all requirements. The system will provide methods of communication between advisors and advisees that keep records of conversation for reference.

Having all this information in one place and its dissemination handled mostly electronically raises a privacy concern. Should the privacy of information be compromised, there is the potential that much more information about a person would be vulnerable. Also if a situation arose where information was released when it shouldn't have it is likely that the error would not be recognized for some time (given the lack of human oversight of information transactions) Without humans overseeing the handling of this information it is important that the way privacy is enforced electronically match legal requirements and user expectations. Likewise, it is important that the way privacy is enforced is described in such a way (and open to modification in such a way) that users understand it. We will therefore be investigating university regulations on privacy of

student records and the opinions of groups (students, advisors, administrators) who will use the new system and currently work with the old one.

1.2 Goals

Our goal is to form a description of how users think about privacy policies in the case of student records. Specifically, we are interested in two questions.

1. What errors do people make when describing privacy requirements (i.e., do they forget key requirements or make incomplete descriptions)?
2. Can we identify any trends in the methods people use to formulate privacy requirements and therefore identify an intuitive representation of policies?

2. Background

There has been a great deal of work done on the topic of privacy, primarily in the fields of psychology and law. Because we are working in the context of the Electronic Advising Folder we are primarily concerned with work relating to the educational setting.

2.1 Privacy in the Information Age

Privacy is complicated by the sheer abundance of information available. Information has become a valuable commodity. This increases the likelihood that personal data may be compromised. You may consent to the supermarket storing data on your shopping habits in exchange for a discount. But that information has value on a secondary market. Maybe advertisers are interested in your shopping habits as well. It is likely that the supermarket would want to take advantage of the opportunity to profit off the information they gathered. The information age has opened up the market for pieces of information that are smaller than ever.

2.2 Psychology of Privacy

2.2.1 What is Privacy?

The longest surviving view of privacy is that of the limited access view, which emphasized how individuals and groups regulate access to themselves (Margulis, 2005). The benefit in maintaining desired levels of privacy is that provides opportunities for self-assessment and experimentation. Relaxation, being one's self, and coping with stress and sorrow are opportunities which privacy allows for us (Margulis, 2005). Margulis draws on Westin's views, relating privacy to control over transactions. In this sense, privacy allows to increase efficiency of information flow while minimizing the risk that the information could be mishandled (Margulis, 2005).

2.2.2 Reasons for Privacy

Margulis defines two different loses of privacy: invasion which is brought on by privacy not initially being achieved, perhaps leaving a form in the open, and violation which occurs when our personal information is disclosed from confidants to third parties. Invasions and violations can both carry a 'cost' depending on what information may then be mishandled.

Privacy can also carry a cost when overexerted. For example, a student that requests their records be completely confidential will find it difficult to prove their attendance or even prove they have been awarded an intermediate degree. The gain from allowing some records to be released is that it allows for actions that are prevented by overzealous guarding. This idea follows from Coleman's definition of trust. Coleman also addresses that if the trustee is trustworthy, then the trustor is better off to give this trust (Coleman, 1990).

2.2.3 How people think about Privacy

The general supposition of psychology is that people are rational beings. However, evidence has been unsupportive and seemingly inconsistent. Kahneman and Tversky (Tversky, 1981) noticed that people are more comfortable with sure gains as opposed to appropriately weight 'risky' gains, such as a "double or nothing". However, when losses were investigated, the sure loss was less appealing than the appropriated 'risky' loss.

Kahneman and Tversky also demonstrated that thoughts and ideas that were more 'available' were likely to be overweighed (Tversky, 1973). Although this was first believed to weigh on concepts that were more frequently talked about and our organizational patterns (e.g deciding if more words began with 'k' or had 'k' as the third

letter), Reyes et al demonstrated that vividness also played a role (Reyes, 1980). For instance, in judging a person's guilt of drunk driving, a more descriptive presentation of the facts could influence the verdict. A description by the prosecution that a defendant had staggered and knocked something to the ground was not as powerful as describing that the bowl, full of guacamole, and fell onto a white shag carpet (Schneier, 2007).

The effects noted by Kahneman and Tversky are but a few of a large set of heuristics that the human mind uses. It is not effective to discuss them all in detail. Bruce Schneier interpreted and categorized how judgment is affected by these heuristics by applying broader definitions (Schneier, 2007). In short, people tend to exaggerate risks that are seen as 'new', 'rare', 'spectacular', 'personified', and 'beyond their control' while downplaying the opposite. In addition to this, Jean Camp has also shown that when placing trust, people are more forgiving of infractions due to incompetence than they are of infractions due to malevolence (Camp, 2006).

2.3 Privacy and the Law

Federal and state constitutions (in the United States) generally don't contain any specific protections of privacy. However, in many cases the bill of rights has been used to protect the privacy of citizens. There have been specific cases were explicit protection of privacy rights have been necessary and laws were created. The most pertinent example of this is FERPA.

2.3.1 FERPA

The Family Educational Rights and Privacy Act, also known as the Buckwell amendment, was created to protect the rights of students attending schools that receive government funding. It was designed primarily to prevent two problems: the first where

students could not view or challenge the contents of their academic records, the second where third parties had too much access to student records (Toma, 1999). FERPA regulations apply to schools that receive government funding in some way, and it provides protection for the privacy of records maintained by those schools.

What Rights are Protected?

Eligible students (and in the appropriate cases their parents/guardians) have the right to review their academic records. They also have the right to challenge the contents of their records (to have information changed or deleted) and the school must provide a process to accomplish this. Students have the right to have their personally identifiable information private from unauthorized third parties. They also have the ability to grant access to this information by submitting consent in writing.

Who is Covered?

Any school, private or public, that receives federal funds is subject to the regulations in FERPA. These funds could come directly from the government or be paid to the school by another (for example a student who pays tuition with some of the money from a federal grant).

Any student of a school, past or present, is covered by FERPA. The parents of the student originally have the rights and protections given in FERPA. When students become "eligible", that is, reach the age of 18 or become enrolled in a postsecondary institution, the rights of their parents transfer to them. The exception to this case occurs when the student is a legal dependent: in this case, their parents retain the right to inspect the student's records. Over forty percent of college students applying for federal aid using FAFSA (Free Application for Federal Student Aid) are classified as dependents

("Number of FAFSA…", 2008). While they have rights under FERPA their parents retain the right to inspect their records.

What is an Academic Record?

FERPA defines an "educational record" as any record kept by the school or by an agency on behalf of the school that directly relates to the student. There are exceptions to this definition. A record kept in the sole possession of the creator used as a memory aid is not included. Records kept by a law enforcement unit of the school are not covered. Some employment records are not covered. If the student is over 18 then records created by a professional (physician, psychiatrist, etc.) are not included. In addition any records that contain only information about the student after they left the school are not covered.

What Protection do these Records Have?

In terms of how these records are protected, FERPA defines "personally identifiable information". This includes the student's name or address or the name or address of any family members, any identifying numbers (such as a student number), or in general any information that would make the student's identity easily traceable. In general the only way for someone to see this information is if the student gives written consent. However, there are cases where the school can disclose personally identifiable information without consent (not that they are forced to do so):

- The school can disclose the information in the form of a directory (with some restrictions).
- The information can be disclosed to other school officials.
- It can be disclosed in the case of a legal investigation.
- Information can be disclosed for the purpose of a study.

- It can also be disclosed for the purpose of determining eligibility for financial aid.

All attempts to access the information by third parties needs to be logged and all the actual access to the records needs to be logged as well (Cate, 1997).

2.4 Electronic Advising Folder Perspective

To gain background on the Electronic Advising Folder we interviewed faculty and staff at WPI who either would be using the system or helped design or implement it in some capacity.

2.4.1 EAF Design

Professor George Heineman was one of the lead members of the team designing the Electronic Advising Folder. We interviewed him for his unique perspective on the system and his knowledge of the various challenges faced during the design.

Most of the design work focused on how to include all the features that they wanted to be able to provide to the students and faculty who would use the system. However particular effort went into deciding how the privacy of certain new features should be handled, such as the 'blog' interface that allowed advisors and advisees to send messages back and forth. Specific issues considered included how the privacy of the messages should be set and who was allowed to configure message settings. They also had to decide how the privacy of the messages would be handled when the advisor was replaced by another either because the student changed majors or the advisor went on sabbatical. Also there was the possibility of a student having multiple advisors or advisors for projects able to see portions of their folder. The designers therefore had to decide how those advisors would relate (in terms of control and access to the folder) to the primary advisor.

2.4.2 EAF Implementation

After design work was completed by Professor Heineman and the Committee on Advising and Student Life (CASL), Roger Donahue took over. Roger is in charge of implementing the Electronic Advising Folder system according to the design. He had to worry about things that are more implementation specific rather than design considerations. Roger's primary concerns were how he would implement the system accurately within the constraints of the software he was using to build the system, and that the system would be able to be maintained in the future by himself or other staff who needed to make modifications to the system.

Most of the system fit well into the existing software but some features of the design required more robust programming. Also Roger needed to choose between "cool" features and the ability for the software to be maintainable and upgradable as staff and tools change in the future.

Roger elaborated on the many privacy concerns with electronic data that aren't as much of a problem in paper. One problem is the ability for people to copy electronic data with ease or store it on portable media and take it with them outside of the systems controls. There was also the problem of how to present the privacy settings to users understandably. It is important that users understand the implications of their choices.

Whenever problems like these came up that could not be easily resolved, the problem was presented to the administrators who would have the final decision on how the problem was resolved.

3. Methodology

Our work focused primarily on interviews with future users (students, advisors, administrators) of the Electronic Advising Folders. During these interviews we wanted to elicit three major categories of privacy information: Roles (the types of users that will use the system), Resources (the kinds of information that is handled), and Release (the methods used to distribute rights to information). The design of the interview was based on our background research into the legal requirements for privacy in this area and our research on the psychology of privacy.

3.1 Interview Design

Users are the most important part of our project. Without them we could provide recommendations for a privacy policy that would satisfy the law, but would be no closer to determining how users understand that policy or how to effectively provide for users to specify their own policy. During the interview subjects are provided with a list of information that might be included in an implementation of the Electronic Advising Folder. This list was compiled from items of information that would be considered part of an academic record according to FERPA, along with information specific to the Electronic Advising Folder (such as notes to and from the advisor and course schedules). In addition to the information that may be stored in the Electronic Advising Folder there is a list of groups and people who may be granted access to some portion of the folder. The specific items on this list can be seen in Figure 1.

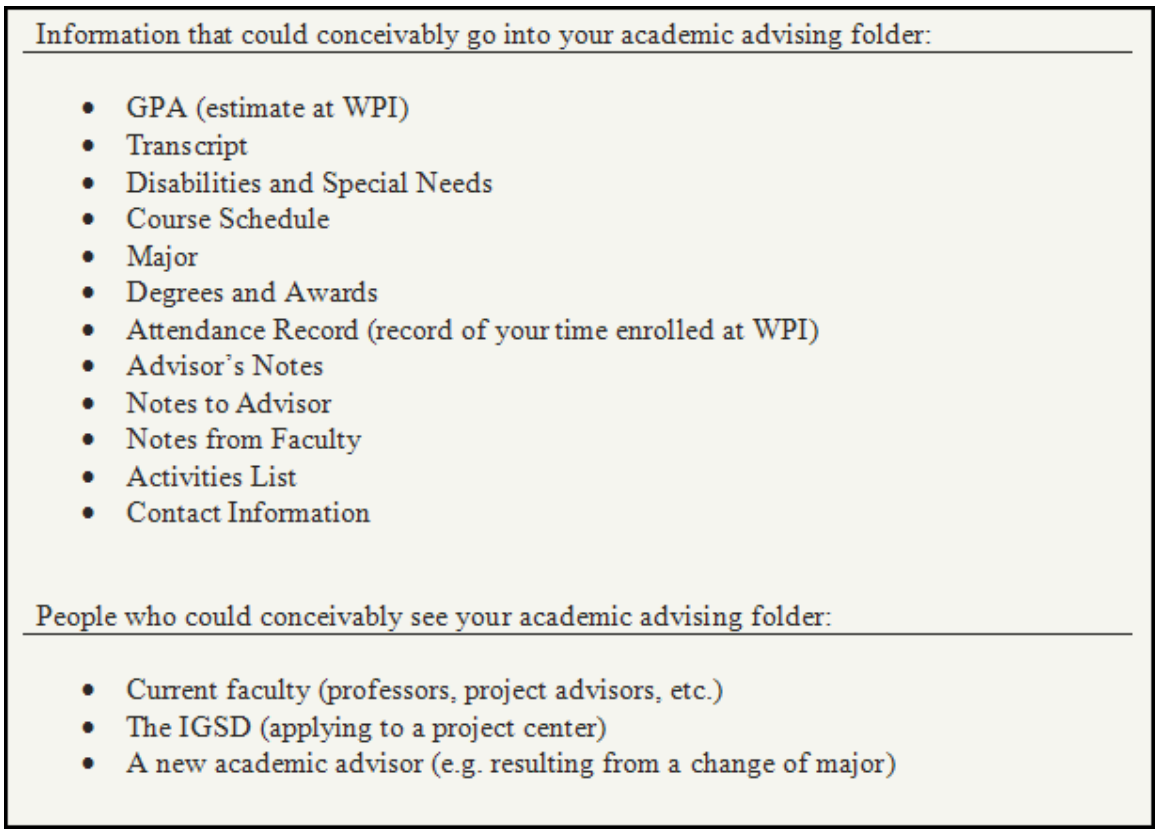

Figure 1: Handout provided to subjects detailing items in EAF.

3.1.1 Prompting

An important part of our interview with users will be prompting them for certain types of responses. Aside from the usefulness of prompts to get the subject talking they are also good for priming certain types of responses. We wish to determine how the user thinks about the privacy policy, specifically how they list and categorize the restrictions. Users might list roles and the varying rights they would have to information, or they might list restrictions on the items of information themselves, or they could describe a policy with a series of access scenarios and the expected results. To determine if there is a tendency to use one method over another we designed prompts that prime users to respond in a certain format and we watched to see if they deviate from that format during the interview. The instructions for interviewers including the prompt questions can be

seen in Figure 2 where the prompts designed to prime for a certain response are given in the white boxes.

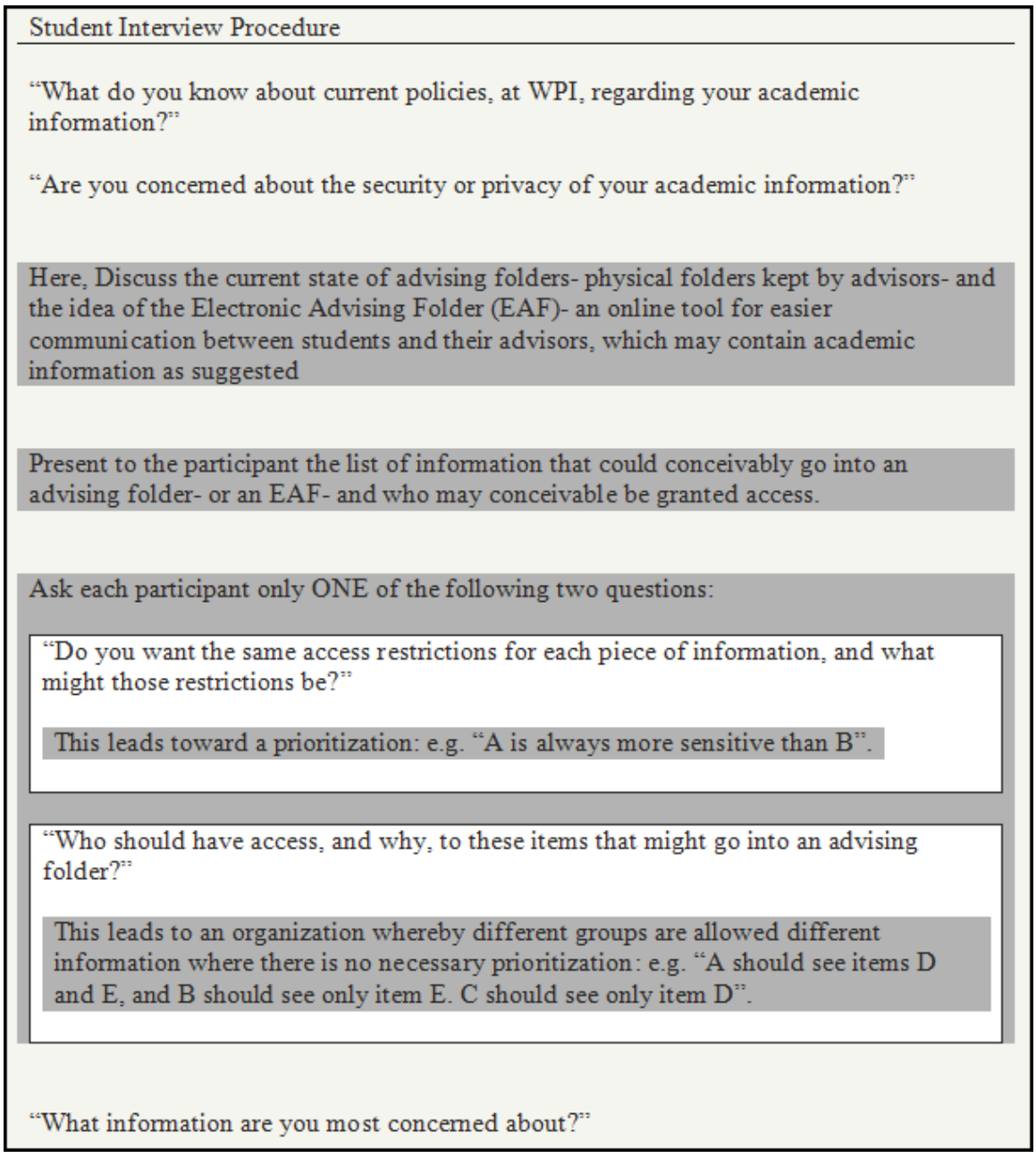

Figure 2: Interviewer Instructions.

3.2 Volunteer Selection

Volunteers were selected from our friends and roommates as well as from emails sent to undergraduates at WPI and messages posted to class message boards. However

these later methods yielded few subjects. An email survey version of our interview was also emailed to students in a “Social Implications” class at WPI.

3.3 Data Handling

Interviews were recorded on a digital voice recorder. They were then transferred to computer and encoded into mp3. The digital audio files were transcribed and both the audio and transcription were put in password protected zip files and stored on a network drive shared by the researchers.

4. Analysis and Results

The goal of this study is to identify possible trends that help define how the participants thought about their privacy requirements. There were a total of nine student interviews that we analyzed, as seen in Table 1. The average length of an interview was about 7 minutes 40 seconds. The shortest was 4 minutes and the longest was 15 mintues.

Table 1: Summary of Participation Figures

Student Interviews	9
Student Email Survey Responses	3
Faculty/Staff Interviews	3
Total	15

4.1 Analysis of Interviews

The most direct form of asking students about their privacy requirements is simply to ask them who, among different types of faculty and administrators, should have access to which pieces of their academic information. The different prompts were used to minimize bias towards or away from using a "clearance level" design. If students still show an overall preference regardless of their prompt, we would have identified a favorable method for participants to think about privacy issues.

Table 2 presents how students in both groups (group A received the classification prompt, group B received the prioritization prompt) wanted each piece of academic information handled by different parties. This has been broken down into how many "Gave/Denied Access" to a particular item, as well as those who reached "No (final) conclusion" and those who had "No mention" of the item. It has also been noted where a participant believed individual students should be able to further tighten or loosen access restrictions by their own accord.

Table 2: Summary of Interview Data by Prompt

Item	Advisor Access	Faculty Access	IGSD/Project Advisor Access
Activities	A Group: 3 Gave Access B Group 3 Gave Access 1 No conclusion (2 For Student Preference to change)	A Group: 3 No mention B Group 2 Gave Access 1 Denied Access 1 No conclusion (2 For Student Preference to change)	A Group: 1 Gave Access 2 No mention B Group 3 Gave Access 1 No conclusion (2 For Student Preference to change)
Attendance	A Group: 3 Gave Access B Group 3 Gave Access 1 No conclusion (2 For Student Preference to change)	A Group: 3 No mention B Group 3 Gave Access 1 No conclusion (2 For Student Preference to change)	A Group: 1 No conclusion 2 No mention B Group 3 Gave Access 1 No conclusion (2 For Student Preference to change)
Contact Information	A Group: 3 Gave Access B Group 3 Gave Access 1 No mention (3 For Student Preference to change)	A Group: 3 No mention B Group 3 Gave Access 1 No mention (3 For Student Preference to change)	A Group: 3 No mention B Group 3 Gave Access 1 No mention (3 For Student Preference to change)
Degrees & Awards	A Group: 3 Gave Access B Group 2 Gave Access 1 No mention (3 For Student Preference to change)	A Group: 3 No mention B Group 2 Gave Access 1 No mention (3 For Student Preference to change)	A Group: 3 No mention B Group 2 Gave Access 1 No mention (3 For Student Preference to change)
Disabilities/Special Needs	A Group: 2 No conclusion 1 For Student Preferences only B Group 2 Gave Access 1 Denied Access (3 For Student Preference to change)	A Group: 2 Gave Access 1 For Student Preferences only B Group 2 Gave Access 1 Denied Access (3 For Student Preference to change)	A Group: 2 No mention 1 For Student Preferences only B Group 2 Gave Access 1 Denied Access (3 For Student Preference to change)
GPA	A Group: 3 Gave Access B Group 3 Gave Access (2 For Student Preference to change)	A Group: 2 Denied Access 1 No mention B Group 3 Gave Access (2 For Student Preference to change)	A Group: 2 Gave Access 1 No mention B Group 3 Gave Access (2 For Student Preference to change)

Item	Advisor Access	Faculty Access	IGSD/Project Advisor Access
Major	A Group: 3 Gave Access B Group 4 Gave Access (2 For Student Preference to change)	A Group: 1 Gave Access 2 No mention B Group 4 Gave Access (2 For Student Preference to change)	A Group: 3 No mention B Group 4 Gave Access (2 For Student Preference to change)
Notes (from Advisor, to Advisor, or from Faculty)	Discussed Separately	Discussed Separately	Discussed Separately
Schedule	A Group: 3 Gave Access B Group 3 Gave Access 1 No Mention (2 For Student Preference to change)	A Group: 1 No conclusion 2 No mention B Group 3 Gave Access 1 No Mention (2 For Student Preference to change)	A Group: 1 No conclusion 2 No mention B Group 3 Gave Access 1 No Mention (2 For Student Preference to change)
Transcript	A Group: 3 Gave Access B Group 4 Gave Access (2 For Student Preference to change)	A Group: 2 Denied Access 1 No mention B Group 4 Gave Access (2 For Student Preference to change)	A Group: 2 Gave Access 1 No conclusion B Group 4 Gave Access (2 For Student Preference to change)

4.1.1 Interview Responses

Of the nine students whose interviews were used, five received the prioritization prompt ("Do you want the same access restrictions for each piece of information…") and the other four received the classification prompt ("Who should have access to…"). Student's knowledge of WPI's policies regarding their academic information was limited. Either the subject claimed to know "nothing" of the policies or they made a general statement that certain information could be released with their permission or that their parents could see some information. One subject thought that information could likely be released in a judicial circumstance.

Prioritization Prompt

All of the subjects except for one specified information-centric descriptions of privacy restrictions. However, most (three of the remaining four) of those subjects also used some level of classification in their descriptions as well. It seems the prompt served to focus them on the important level of the information, but was not sufficient to completely remove the tendency to specify restrictions by group or individual. All of the subjects mentioned the need for Disabilities and Special Needs information to be restricted.

Classification Prompt

All but one of the subjects given the classification prompt specified groups of people or individual people who needed to/should have access to portions of the advising folder information. However, most (three of the remaining four) of these subjects also mentioned specifically the importance of the Disabilities and Special Needs information and said access to it should be restricted.

Those subjects who assigned rights to groups and individuals used three general methods for specifying restrictions. The first was to consider the needs of the group to perform its function (such as the IGSD needing access to certain information in order to do their job). The second method for determining rights was to consider the implications if a group were to have access to information (namely the negative consequences. This method focused on hypotheses like: “Professors might be biased if they knew a student had a low GPA or had been at school for much longer than the normal amount of time”, or “Students might not want their parents to know if they are not doing well”. The final method seemed to be based on how much the subject trusted the group or individual. Subjects would give the broad right of access to the entirety of the information; however

this was only in cases of the advisor or their parents. The first method was only (obviously) seen in two interviews. However, the later two methods were noticed more often (the second method four times, and the third method three times).

4.1.2 Email Responses

A class of undergraduate students was given the opportunity to take a survey consisting of the text of our interview. Although six students expressed interest in the survey, only three returned the completed document. Of the three surveys returned 1 was the prioritization prompt ("Do you want the same access restrictions for each piece of information…") and the other 2 were the classification prompt ("Who should have access to…").

The students' knowledge of the current policies at WPI regarding their academic information was limited, however this could be a result of the survey not properly encouraging the students to fully elucidate their knowledge of policies (because all students meet with their advisor on academic advising day they presumably know that their advisor could access at least some of their academic information, yet only one student explicitly mentioned this). Only one of the students mentioned that they knew parents of dependent students could see academic information despite a recent change in WPI policy whereby all undergrads are considered dependent until they file a form proving otherwise. One student mentioned that information could be released on a "legitimate 'need-to-know' basis", however they did not elaborate on what would constitute a legitimate request in this case.

All the respondents mentioned that they were concerned about the security of Disabilities and Special Needs information.

Prioritization Prompt

The student that received the prioritization prompt responded that their advisor should have access (presumably to all the listed information) because they would be unable to do their job (of advising) otherwise. They also mentioned that applying to do a project with the Interdisciplinary and Global Studies Division (IGSD) is like applying to a job and therefore the IGSD should have access to the information of students who apply. The student did not seem to be lead by the prompt and rather formed the two groups of "who has access", the advisor and occasionally the IGSD, and "who doesn't have access", everyone else. This could be due to the fact that possible groups of people who could see academic information were listed on the survey.

Classification Prompt

Of the two students who received the classification prompt one wanted the notes to and from their advisor to be restricted to just their advisor and themselves. They also didn't want anyone to have access to the disabilities and special needs information. The other student's response was closer to that of the prioritization prompt student's. They specified that only their advisor should have access to the information in their folder unless they specifically allow others (such as current professors or potential project advisors) to see certain information.

There is a difference in the way these two students handled the prompt. The first student identified individual pieces of information in the folder that they considered important and specified who should have access to them. This could be motivated by the student's notion of how sensitive each piece of information was. The second student, similar to the prioritization prompt student, specified their restrictions in terms of broad categories of who should and shouldn't have access to their information. This method

seems to be centered around the individuals and groups who might have to have access to their academic information rather than the information itself. Neither student mentioned anything about intermediate groups who might have access to a limited set of information besides the second student's exemption that students could grant access to parts of their folder.

5. Conclusion

The only cases in which subjects left out restrictions on important information (i.e. made an error in their policy description) was when they were apathetic about that information. We found much more interesting information when it came to how people chose to reason about and represent their privacy requirements. It was clear from the interview data that subjects did follow the prompts to some extent. More important however, was that subjects in both groups used similar techniques relying on both forming groups with rights to information and assigning importance levels to pieces of information themselves. The prompt towards classification for example, was able to bias subjects towards this method, however subjects still emphasized the importance of the Disability and Special Needs information regardless of the groups or individuals involved. Likewise the prioritization prompt resulted in policy descriptions much more information-centric, however subjects still used groups with rights in their policy. It seems from the results that both these methods are intuitively useful by the general public and some mix of them is appropriate when forming policy descriptions.

Ultimately if we wish to reconcile possible differences between human interpretation and computer-evaluated policies we will need to use more formal tools. The interview format is useful for gaining a broad picture of how people think about privacy policies and getting some idea of how they may reason about these, but it is difficult to make more precise observations. More rigid surveys of how people reason about privacy policies would be useful. For example, giving people a real privacy policy and asking them to interpret it might show where common mistakes are being made. Also it would be useful to look at how the content of policy description influences the resulting

policy. For example, subjects in our study were obviously limited in some way by the choices of what people and information to tell them about. One final suggestion is that while it is reasonable to assume that people would understand a policy better if it was presented in a manner intuitive to them, it may not be best to have them specify their own policy in the same way. It is possible that by forcing people to specify privacy requirements in a more "uncomfortable" manner they may produce a more rigorous policy that is more true to their actual desires. The opposite could be true as well, but this is worth mentioning as we think it would be hasty to assume the most intuitive method of presentation is also the method best used to produce a policy as well.

Bibliography

Bairu, Ghedam. “Forum Guide to Protecting the Privacy of Student Information.” National Center for Education Statistics: 2004

Camp, L. Jean, Cathleen McGrath, and Alla Genkina, “Security and Morality: A Tale of User Deceit”, Models of Trust for the Web MTW’06, (Edinburgh, Scotland) 22 May 2006.

Cate, Fred H. “The Privacy and Security Policy Vacuum in Higher Education.” Educase Review 41.5(2006): 18-28.

Cate, Fred H. Privacy in the Information Age. Harrisonburg, VA: R.R. Donnelley and Sons, 1997

Cheung, Oona, et al. “Protecting the Privacy of Student Records: Guidelines for Educational Agencies.” National Center for Education Statistics, NCES-97-527: 1997

Coleman, J., 1990 Foundations of Social Theory, Belknap Press, Cambridge, MA.

“Family Educational Rights and Privacy Act Regulations.” 23 May. 2006. U.S. Department of Education. 10 Sep. 2007. <http://www.ed.gov/policy/gen/reg/ferpa/index.html>

Kahneman, Daniel, and Amos Tversky. “Prospect Theory: An Analysis of Decision Under Risk.” Econometrica 47(1979): 263-91.

Kaplin, William A. The Law of Higher Education. San Franciso: Jossey-Bass, 1978

Margulis, Stephen T. “Privacy and Psychology.” Presented at Contours of Privacy: Normative, Psychological and Social Perspectives(2005)

“Number of FAFSAs received by state for 2006-07 and 2007-08.” 26 Feb. 2008. National Association of Student Financial Aid Administrators. 6 Mar. 2008. <http://www.nasfaa.org/publications/2008/eafafsabystate022708.html>

Plous, Scott. The Psychology of Judgement and Decision Making. McGraw-Hill, 1993

“Protecting the Privacy of Student Education Records.” National Center for Education Statistics, NCES-97-859: 1997

Reyes, Rober M., William C. Thompson, and Gordon H. Bower, “Judgmental Biases Resulting from Differing Availabilities of Arguments”, Journal of Personality and Social Psychology, 1980, 39:2-12.

Schneier, Bruce. The Psychology of Security. 28 Feb. 2007. 10 Sep. 2007. <http://www.schneier.com/essay-155.html>

Schwartz, Barry. “The Social Psychology of Privacy.” The American Journal of Sociology 73.6(1968): 741-52.

Slovic, Paul, Baruch Fischhoff, Sarah Lichtenstein. “Rating the Risks.” Environment 2(1979): 14-20, 36-39.

Slovic, Paul. The Perception of Risk. Earthscan Publications Ltd, 2000.

Steinfeld, Lauren, and Kathleen Sutherland Archuleta. "Privacy Protection and Compliance in Higher Education: The Role of the CPO." Educase Review 41.5(2006): 62-70.

Toma, J. Douglas, and Richard L. Palm. 1999. The Academic Administrator and the Law. ASHE-ERIC Higher Education Report Volume 26, No. 5. Washington, D.C.: The George Washington University, Graduate School of Education and Human Development.

Tversky, Amos, and Daniel Kahneman, "Availability: A heuristic for Judging Frequency", Cognitive Psychology, 1973, 5:207-232.

Tversky, Amos, and Daniel Kahneman, "The Framing of Decisions and the Psychology of Choice", Science, 1981, 211: 453-458.

Tversky, Amos, and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases." Science 185(1974): 1124-30.