The Effects of Introspection on Computer Security Policies

Stephanie A. Trudeau

Senior Honors Thesis
Advisors: Sean Smith, Scout Sinclair

Department of Computer Science

Dartmouth College
Hanover, New Hampshire
June 3, 2009

Stephanie.A.Trudeau.09@alum.dartmouth.org
Abstract

What does it mean to be an expert? And what makes an expert more capable than a non-expert when it comes to evaluating and articulating their impressions about something as commonly practiced as food tasting? How do we explain those behaviors that humans perform very well, but don't quite know why? Studies have shown that there exists a class of activities that we as humans execute well intuitively, but that we perform much worse upon introspection. Evidence supports the claim that the act of introspection actually causes us to do more poorly at these tasks.

My goal is to apply this idea to computer security. At present, designs for most security policy interfaces leave much to be desired. This lack of usability leaves these systems in need of improvement, possibly causing users to become more vulnerable than they otherwise would have. My research includes a user study on the privacy policies of the interface for a social networking website similar to Facebook. Evidence from the study supports the claim that the act of introspecting upon one's personal security policy actually makes one worse at making policy decisions.
Acknowledgements

This thesis is the culmination of nine months of research and work, however, I consider the past four years of my education to have been crucial in preparing me for the work that I was able to accomplish in this document. I would like to extend my gratitude first to Paul Christensen, who always encouraged me to choose my major based on what would make me happy in life. Next I must thank Tom Cormen, who inspired me to believe that Computer Science could be that major, and who has personally helped me through many of the struggles that came from switching to a CS major with no experience in the field. Without his support I never would have envisioned myself ending up where I am today, as I complete this senior thesis in Computer Science. Next I must thank my thesis advisor, Sean Smith, who was my first introduction to the world of research as well as to computer security and usability. I have greatly enjoyed the past three years of work I have done with Sean, and will never forget the many lessons he has taught me, both about academics and about life. I could not have asked for a more understanding advisor, and I know that there were times that I only made it through because of Sean's confidence that I would, for which I will always be grateful. Next I must extend my gratitude to Scout Sinclair, who has mentored me greatly over the past three years. She has supported and encouraged me through many of my toughest moments in my education, and is certainly partially responsible for my making it to the end of my time here at the college on the hill. Additionally, I wish to thank all the graduate, doctorate, and post-doctorate students I have known in the PKI Lab during my time at Dartmouth—namely Pete Johnson and Chris Masone. Seeing other successful people who have made it beyond where I am has given me hope during the times when I needed it most. Your friendship and the conversations we have shared have also meant a lot to me, and have inspired me to want to continue with my own education.

I would also like to thank Denise Anthony and Deanna Caputo for all their help in designing my user study, and in particular Denise for all the knowledge and help she gave us as we were analyzing our results from the user study.

Finally, I would never have been able to complete this thesis without the love and support of my family and friends. My loving parents, Brian and Melinda, have been the
most supportive and encouraging voices in my life, and deserve the credit for every accomplishment I have ever received. I am extremely grateful for all the wisdom that they have imparted upon me, and am well aware that I would never have made it this far in life without their unfaltering belief in me and my abilities.

As for my friends, you are the most tangible support I have had in my time here at Dartmouth. I'd like to personally thank Chase Decker, Sehwan Ahn, Jack Bowman, Michael Diamond, Lelia TahaBurt, Michelle Earhart, and E McNeill for their wonderful comraderie over the past two terms. You have kept me sane during times I thought I would never survive, you have provided me the outlet to release my creative energy and excitement, and you have helped teach me more about myself. I would not be the same person had I not met any of you, and I would not have had the most amazing senior year I could have were it not for each of you. (I also wouldn't be a nerd if it weren't for you guys.) Thank you for being the reasons I wish I weren't leaving Dartmouth yet. A special thanks goes to Jack, Michelle, and Chase for being my research assistants while I was conducting my user study; you made that week so much more enjoyable for me! And lastly, I'd like to especially thank Chase for being the best friend I've ever known. Your thoughtfulness never goes unnoticed, the support you have provided me over the past two terms has been irreplaceable, and your loyalty will never be forgotten. I would not be crossing that stage to receive my diploma without you.

And to all others whom I have not mentioned here, but have provided me with the support and the means to arrive in the place where I am today, I thank you.

This research was supported in part by the Institute for Information Infrastructure Protection (I3P) and the U.S. Department of Homeland Security, under Grant Award Number 2006-CS-001-000001. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

June 3, 2009
Hanover, NH
Contents

1. Introduction
   1.1 Real World Examples ................................................. 3
   1.2 Reasons Why Security Breaches Happen .......................... 4
   1.3 Locked-Room Activities and The Jam Test ......................... 6
   1.4 Thesis Statement ...................................................... 8

2. Applications of Security Policy Interfaces
   2.1 File Permissions ....................................................... 9
   2.1.1 The Expandable Grid: A study of policy authoring .......... 11
   2.2 Email Clients .......................................................... 12
   2.2.1 ABUSE: A study of email trust relations .................... 12
   2.3 Web Browsers .......................................................... 14
   2.3.1 HTTP Cookies ....................................................... 15

3. Selecting a Problem to Study
   3.1 Requirements of the Study ......................................... 18
   3.2 A Model for the Study ............................................... 20
   3.3 Web browser User Studies ......................................... 23
   3.4 File Permissions User Studies .................................... 26
   3.5 Email User Studies ................................................... 30

4. The User Study
   4.1 Subjects and Recruitment .......................................... 32
   4.2 Part I – The Questionnaire ......................................... 33
4.3 Part II – InnerCircle .................................................. 34
4.4 Experimental Hypothesis .............................................. 37

5. Results

5.1 Original Hypothesis .................................................... 39
5.2 Analysis of Results ..................................................... 40
5.3 Possible Explanations .................................................. 48
5.4 Future Work ............................................................ 50
Chapter 1

Introduction

Policy interfaces are a vital component of securing a large array of applications. Web browsers, online social networks, file systems, online health databases, and email clients are all examples of systems containing data that needs to be secured. When the information managed by any one of these systems is compromised, the repercussions to the user have the potential to be quite costly financially, physically, and emotionally. Due to the serious nature of this risk, developers have worked to ensure that the security component of all such applications is fully functional and that the user is able to configure their security settings to allow any type of behavior they wish for their data. But these security mechanisms will only work if they are used correctly. In the words of Whitten and Tygar,

“Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the Encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or
accidentally configure their access control mechanisms to make their private data world readable” (170).

In other words, a security system that is securable in theory is of no use unless it is actually secure in practice (Tognazzini 31).

The emerging field of Human-Computer Interactions and Security (HCISEC) focuses on this challenge. HCISEC researchers work to infuse usability with security in the hope that the design of security systems will consequently become more secure when actually used. Many in the field are grounded on the principle that humans are (and should be) playing a role in security tasks, which means that computer security is sociotechnical in nature (Masone 1). For this reason, HCISEC researchers attempt to employ knowledge from various fields in the social sciences, such as psychology, sociology, or economics. HCISEC experts remain optimistic that this approach will help to determine both why current security systems are failing to do their job and what standards might resolve these issues (Masone 1).

While many are working hard to remedy the inadequacies of policy-authoring interfaces, there are still many who do not recognize the current problems in this area. Computer experts often assume that perfectly secure systems already exist. However, the demand for more usable security policy interfaces is constantly increasing, along with the tendency for computing to become more collaborative and distributed. Predictably, as more applications become increasingly complex, the opportunity for misuse of the data they handle also rises. This in turn drives up the need to build policies that will prevent abuse of the data contained within these applications (Reeder 3).
With the increasing opportunity for misuse also comes the expanding knowledge of how to do so. Kevin Mitnick, a famous computer hacker, confessed that he rarely needed to crack a user’s password because it was simply easier to fool them into revealing it to him (Sasse 13). Computer hackers are constantly honing their skills and developing more elaborate and inaudible attacks. As security measures become more elaborate and comprehensive, so too do the attacks of those with malicious intent. Furthermore, the number of computer experts is not increasing at the same rate as the advancement of these security systems. This means that the burden for managing security policies is beginning to rest upon the non-technical end-user (Reeder), rather than the designer. It has become the case that each day the need to develop truly usable security policy interfaces is more important than the day before.

1.1 Real World Examples

In spite of the fact that businesses continue to increase their spending on security products, the number of businesses that are experiencing breaches of their security is still continuing to increase rapidly. In 1998, 32% of the United Kingdom businesses that were surveyed by the UK’s Department of Trade and Industry had experienced a security incident. In 2000 this number rose to 44%, in 2002 it reached 74%, and in 2004 it became a monstrous 94% (Sasse 14). These numbers prove that the security crisis is very real and needs to be addressed.

In 2001, a major security breach in the United States Senate Judiciary Committee occurred, later to be known as the Memogate scandal. A Republican staffer on the Committee discovered that he had the ability to read confidential memos and many other
documents belonging to the Democrats serving on the Committee. This obvious mistake was made possible by the use of a shared file server. The Committee’s new system administrator had accidentally set the default permissions on new directories to be “public,” rather than password-protected. No special access rights were required for the staffer to access these files. Anyone could do so by following the path “My Network Places > EntireNetwork > Judak” (Gehringer).

1.2 Reasons Why Security Breaches Happen

According to Sasse and Flechais, there are four main reasons why users share their passwords, fail to encrypt their private messages, and turn virus checkers off. They say that most users:

• Are unable to use security tools correctly
• Fail to grasp the importance of data, software, and systems in their organization
• Do not believe that they personally will be attacked
• Do not realize that their behavior is putting their assets at risk. (13)

These can be boiled down to two reasons why users fail to demonstrate secure behavior; either they are unable to behave in the way that is required or they do not wish to comply with the behavior that is required.

Why is it that users do not behave as required for maintaining their security? With such serious consequences, one would think that there is very strong motivation to do so. Part of the problem is that users have a multitude of passwords, for everything
ranging from logging into their email account to opening the locked door at their work to withdrawing money from their bank account at an ATM. Some of these passwords are used daily, but others are used infrequently. Many passwords are required to change on a regular basis. Some passwords are required to include numbers, exclude words, and to use characters other than letters. The demands on human memory make it nearly impossible for the majority of users to provide the memory performance that this requires. (Sasse 17).

Sasse and Flechais provide a great anecdote to illustrate the lengths that users will go to cope with remembering their passwords. They wrote:

> The customer relations manager of a UK building society received irate phone calls after a major re-branding exercise, in which ATMs and the surrounding environments had been restyled. The customers did not object to the new corporate color scheme, but rather, to the fact that the panels and surroundings on which they had written or scratched their PINs had been replaced, and as a result they were unable to withdraw cash. (17)

It is certainly true that requires no use of passwords or authentication would be more usable, but it would not be very secure. A computer that requires a retina scan every ten minutes in addition to a password would be extremely secure, but nobody would choose to use it. It is also true that not using a computer at all would maintain a user’s privacy as well, however this option is also not feasible. Clearly humans need to use computers. If a person cannot find a computer that is secure to use, they will use one that is not.
1.3 Locked-Room Activities and The Jam Test

In his book *Blink*, Malcolm Gladwell discusses the idea of a special type of task which he refers to as a locked-room activity. A locked-room task is by definition one that the user performs well without consciously thinking about it. When questioned, however, about one’s decisions and the reasons behind their actions, a person actually seems to become worse at performing locked-room activities. It may be the case that computer security is one of these locked-room tasks, which would explain why when a user is asked to specify her security policy, she is unable to do so accurately. In general, people have well designed policies in their head, but lack the means with which to implement these nuanced policies (Cranor “Designing”).

Gladwell also discusses what he calls the jam test in his book *Blink*. Taste testing experts have ranked all 44 jams that exist in order from the best to the worst. In an experiment conducted by Timothy Wilson and Jonathan Schooler, college students were asked to rank 5 of these jams (those ranking 1\textsuperscript{st}, 11\textsuperscript{th}, 24\textsuperscript{th}, 32\textsuperscript{nd}, and 44\textsuperscript{th}, according to the experts) in the order they thought tasted the best. The students were divided into two groups. In the first group, students were asked just to rank the jams, but in the second group the students were asked both to rank the jams and to provide a written explanation of why they ranked them in the order they did. The result was that the first group gave a reasonably close list of rankings to that of the trained experts, agreeing on both the best and the worst jams and showing a correlation of 0.55. In contrast, the second group performed much worse in comparison to the experts, demonstrating only a correlation of
“By making people think about jam, Wilson and Schooler turned them into jam idiots” (Gladwell 181).

Gladwell explains that part of the reason for such a poor performance by the second group of student testers is that people do not normally put into words their decision of whether or not a jam tastes good. When they try to do so, they are attempting to measure the jam by a metric that they do not understand. While a taste-testing expert understands the nuances of texture and stickiness and sweetness when tasting a food, a non-expert does not. The attempt to justify their decisions using these unfamiliar metrics causes these inexperienced testers to question their decisions and to try consequently decide on poor choices that seem more justifiable. In essence, these testers are taking a locked-room activity out of the locked room, which destroys their capacity to do well.

We believe that Gladwell’s observations may very well apply to computer security. One of the problems with giving a security policy user the comprehensive dimensions needed to determine a safe security policy is that average users do not understand these dimensions. They are being given all the information they need, but are unable to effectively apply it. As a result of their misunderstandings, users are constantly compromising their own security. “Designing a user interface for specifying privacy preferences is difficult for several reasons: privacy policies are complex, user privacy preferences are often complex and nuanced, users tend to have little experience articulating their privacy preferences, and users are generally unfamiliar with much of the terminology used by privacy experts.” (Cranor, “Designing”).
1.4 Thesis Statement

The objective of this thesis is to test the hypothesis that computer security policy authoring is a locked-room activity. That is to say that computer security falls into the category of activities in which a user’s performance decreases when the user attempts to apply conscious techniques to their policy authoring. We hope to show this by performing a user study that will demonstrate this fact in its results. Establishing this would show security system designers that the current way of designing policy-authoring interfaces is ineffective for non-experts, demonstrating the need to reform security system designs.
Chapter 2

Applications of Security Policy Interfaces

The problem of usable privacy policy interfaces can be viewed through a number of different lenses. Web browsers, online social networks, file systems, online health databases, and email clients are all examples of systems containing data that needs to be secured. In this chapter, we consider three examples of scenarios where these issues are evident—file permissions, email clients, and web browsers.

2.1 File Permissions

The term file permissions refers to the access rights that are granted to individuals or groups of users with regard to a particular file. In the traditional Unix approach, there are three permission settings that must be set: read permission, write permission, and execute permission. For each of these permissions, access may be granted to either an individual user, to an entire group of users, or to all users. Improperly configured file permissions can have severe consequences, enabling misuse by those who were not intended to view, alter, or run certain files.
The Memogate scandal (Gehringer) discussed in Section 1.1 serves as an example of the serious issues that can arise from improperly set file permissions. Another example is the Microsoft NT file system. Maxion and Reeder point out

Microsoft publishes a list of “best practices” for NTFS security that advises users not to use several of the provided features of the NTFS permissions model, such as negative (i.e., deny) permissions and the ability to set permissions on individual files as opposed to folders. The best-practices document states that use of these features “… could cause unexpected access problems or reduce security.”

(26, 27)

Clearly a system that provides such tricky functions is prone to mistakes. If the best-practices document must warn users that they might reduce their security by using a feature, then there certainly must be a better design for the use of that feature. A third example of problems with the usability of file permissions interfaces is in the user study done by Good and Krenkelberg on the KaZaA peer-to-peer (P2P) file sharing user interface. The study concluded that most users could not accurately determine which files they were sharing and which they were not. At times, the users would falsely assume that “they were not sharing any files when in fact they were sharing all files on their hard drive” (137). The analysis of the KaZaA network revealed that several users were indeed capitalizing on these mistakes and downloading files of other users that contained private information.
2.1.1 The Expandable Grid: A study of policy authoring

In 2008, Robert Reeder wrote his Ph.D. dissertation for the Carnegie Mellon University School of Computer Science on the subject of policy-authoring user interfaces. Reeder studied visualization techniques used in these interfaces, and developed his own interface—called the Expandable Grid—to test the techniques he believed were most effective in policy-authoring interfaces. Reeder believed his Expandable Grid would lead to more accurate performance on policy-authoring and policy-viewing of the file permissions on the computer.

Reeder notes that list-of-rules interfaces tend to hide contextual information from the policy author. Users often need this information, however, in order to accurately author their rules. Multiple rules might conflict with one another, or default settings may behave incorrectly for specific scenarios. Users need to see this information, says Reeder, in order to accurately conclude which setting they want in their privacy policy (4). In his Expandable Grid, Reeder made three main improvements based on problems he saw in the Windows XP file-permissions interface. First, he made the interface show the entire privacy policy for every resource and principal, all in one view. Second, he showed the user the “effective policy,” so that they would see the resulting access decisions that were made based on their file permission settings. Lastly, the Expandable Grid showed the combined effect of all the rules (8). Reeder made the claim that his Expandable Grid significantly improved the performance for setting file permissions on a computer.
2.2 Email Clients

Email is another major source of security violations. There is a host of different ways a user can be attacked through their email. A malicious user might try to sniff the packets of information being sent across a network in order to obtain private data that another user has sent via email. A user might receive an email that is a phishing scheme, requesting that they send account, credit card, or other personal information to a fake user impersonating some type of authority. It is also very common for a malicious user to attempt to implant a virus on another user’s computer through an attachment found in an email. “Man in the Middle” attacks are another hazard of using email. In these attacks, an adversary intercepts messages going between two users and injects new messages, or modifies the existing ones, before they arrive to the other user. This gives the illusion to the victims that they are communicating over a secure connection when in actuality they are not (Masone 14).

2.2.1 ABUSE: A study of email trust relations

In 2008, Christopher P. Masone completed his dissertation for a Ph.D. in Computer Science from Dartmouth College on the subject of secure email. He focused on how humans decide to trust new correspondents. Using Public Key Infrastructure (PKI) technology, Masone developed criteria for a system that applies social science research to computing. In his work, Masone defines a “trustworthy email” to be one that exhibits these three properties:
1. **Integrity:** the message has not been undetectably tampered with in transit.

2. **Sender Authenticity:** the recipient can reliably determine that the purported sender of the message actually sent it.

3. **Context:** the recipient can glean enough information from the message to build a shared set of expectations with the sender. (14)

Masone takes on the challenge of building an email system that will take into account the different types of trust decisions that humans must necessarily make while using it. This system must exhibit two new characteristics that other email clients lack. First, it needs to use new signals that are easy for a trustworthy user to apply, but difficult for a malicious user to employ. Second, the system must not introduce any new usability issues than those that already exist. Masone developed Attribute-Based, Usefully Secure Email (ABUSE), which he claims met all the criteria laid out in this section. This assertion is based on two user studies that were performed. Users were placed in a simulated power grid emergency and were required to determine whether or not incoming emails were coming from a trustworthy source. Each of the emails requested that the user perform some action related to the power grid. Subjects were randomly assigned to one of three groups, each of which used either a Plaintext, S/MIME, or ABUSE email client (119). The results showed that both ABUSE and Plaintext users scored much higher in correctly identifying the trustworthy users. A significantly higher percentage of ABUSE users were correct without the use of any outside sources of help, which were allowed in order to make the study more closely resemble a real-world scenario.
However, in untrustworthy scenarios, ABUSE users were no more successful than others (133).

2.3 Web Browsers

Another sizable source of both security and privacy attacks is the World Wide Web. Attackers using this medium will often attempt to acquire personal information from the victims, such as credit card information, account passwords, or social security numbers. Many companies are able to make money by selling the personal information—such as phone numbers or email addresses—that they have gathered on their web site to telemarketers or other companies. Even information that seems nondescript, such as which websites a user has viewed, can be compiled to determine the buying habits of a particular user, her areas of interest, or other information useful for marketing. Advertisements that appear in the user’s web browser can then be tailored toward the interests of that particular user.

Many users are concerned about their privacy online. A 2001 survey conducted by Culnan-Milne stated that 16% of Internet users did not trust a company to follow their privacy policy that they had posted on the web. A 1997 Westin survey stated that 65% of those surveyed indicated interest in a hypothetical free and easy-to-use product that helps them record their preferences for the way they would like their personal information to be used by the web sites of businesses (Cranor, “Web Privacy” 14). Additionally, a 2001 survey by Forrester Research said that 34% of Internet users who do not make purchases online would start buying items online if their privacy was no longer a worry (13). Despite all their concern, however, most users do not seem to exhaust all precautions
before taking action online. In 2001, Harris Interactive conducted a survey of 2,053 adult
Internet users. This survey revealed that a mere 3% of respondents review the privacy
policy of a website most of the time, while 64% said they would only glance at the
privacy notice or avoid reading it altogether (13). Then again, this may be due in large
part to the fact that online privacy policies tend to be wordy and full of jargon.

Mark Hochhauser, a psychologist and linguistics expert, looked at the privacy
policies of ten popular web sites for USA Today and concluded that all were written at a
college reading level or higher. At the time that this article was written, a single sentence
of the policy for HealthCentral contained 174 words. "If you really don't want people to
understand," he says, “write it in legalese and have it run on for four or five pages,”
(Roger). It is unreasonable to expect a normal user to have such a legal vocabulary.
Writing a privacy policy in such complex language is clearly done with the expectation
that users will not carefully inspect the entire policy. Unfortunately, users have in fact
developed this bad habit of skipping over the privacy policy entirely.

2.3.1 HTTP Cookies

“Cookies” have become a buzzword in web privacy discussions as well. Cookies are
an addition to Hypertext Transfer Protocol (HTTP). In a web browser, every link is
identified by a uniform resource locator (URL). When a user clicks on a (hypertext) link
in their web browser, the browser connects to the server that matches the URL embedded
within that link. This means that the web browser sends a request message to this server,
and in turn the server sends a response message. Once the response is received, the
browser disconnects from the server. The browser must make a new connection for each
request, which means that the server handles every request as if this were the first time that a user was trying to make the request. Because there is no connection from one request to another, it can be said that a request is “stateless” (Kristol 152).

This quality of being stateless makes it easier to write a web browser and build a server. Some web applications need this information, though, and are much more difficult to write without a record of the multiple requests to the same server by one particular user. Cookies exist for this reason. A “cookie” is the information that is passed between one’s web browser and the server matching the URL that he is visiting. A web browser will store only the cookies from a server it has visited. One might think, then, that constricting the browser to return a cookie only to the server from which it was received would be a wise security policy setting to have, however, this is actually very restrictive because most large organizations have multiple web servers who all need to share this information (Kristol 154).

Cookies have many uses. They can store a user’s login information for a website so that she need not enter this data each time she wishes to access the site. They can mark which pages a user visits on a particular website, which can be used to determine patterns in how the site is navigated. The website’s makers can then structure the site in such a way that the most popularly viewed information is easiest to access. One concern with cookies, however, is that they are able to travel beyond their intended target. “Third-party cookies” are another cause for alarm. When a browser loads a page from one website and the images (e.g. for an advertisement) from another, it is possible for the latter source to attach a cookie with the image. One can expect a cookie from the first website, but a user would have no reason to suspect a cookie from the second source.
This enables advertisers, for example, to track all sites that a user visits, so long as they have implanted a third-party cookie at each of these sites. An attacker can also hijack cookies that are being sent between the browser and a server by using a packet sniffer. While most web browsers give you the ability to disallow third-party cookies, or to disable cookies altogether, many websites do not run well without the use of cookies. For example, an online shopping website would not be able to use a “shopping cart” feature without the use of cookies.
Chapter 3

Selecting a Problem to Study

In order to effectively study the issues of security policy usability that have been laid out in this paper, the focus will narrow to one of the applications laid out in Chapter 2. All three of these examples provide realistic scenarios in which users must make decisions about their security. Each application also has enough problems that there is room for significant improvements to be made. Additionally, improvement in any one of these areas would benefit users at all different skill levels. However, to gather information that is useful in remedying any of these problems, it will be necessary to take a closer look into one of them individually.

3.1 Requirements of the Study

Practically speaking, there are many restrictions that must be considered when selecting which manifestation of a security policy should be studied. First and foremost, this study has a significant time restriction imposed upon it, as it is being written as a senior thesis. It must be completed within the span of 3 months, but ideally could be
completed in under a month. While this still allows for many possibilities, it does limit the potential for which user studies can reasonably be considered. Another restriction is that this study must be administrable from the Dartmouth College campus. That is to say that it must be conducted either on campus or in some other manner such that the administrator of the experiment is able to remain on campus.

Another consideration is that the actual study should not demand copious amounts of training from the users. While they may be expected to learn a small amount about the task they will be performing or the situation they may be simulating, this training should not be too extensive. Requiring too much education from the user will cause him to lose interest, which will decrease his focus as well as his motivation to do well. Though we don’t want to overeducate the users, we also want to be sure to provide a sufficient amount of training that they should be able to accomplish any of the tasks we assign them to do. While being able to figure out the behavior of a program by oneself is arguably a component of usability, given the time restriction we will be imposing on the study, the user should know everything they need to in order to accomplish the assigned tasks. An important point to consider is the length of the study. If the study is longer than two hours, it should be broken into multiple intervals, so the user is able to stay fresh for the tasks. Ideally, the study would require only one sitting, as this would most likely lead to more willing participants.

Finally, the type of study we choose to do must be one that contains an oracle—an expert baseline that can be considered a perfect security policy. In other words, there needs to be a “right” answer and a “wrong” answer that the user can choose, so that an evaluation of the participant’s performance can be made. It will also be important to
motivate the user. We want the participant to care about doing well, so that they try their hardest as they would in a real-life situation, rather than acting without care because they are just participating in a simulated scenario. Additionally, we must take care to distribute our demographics. Balancing the ratio of males to females is important, as well as recruiting students of varying majors and disciplines, and with a variety of familiarity with computers. This means we will need to make sure that we do not advertise the study to particular student organizations or departments, but rather to the entire student body.

3.2 A Model for the Study

In addition to considering all of the requirements listed in Section 3.1, the user study must also fit the model of what we are attempting to investigate. To establish this model, let us first consider Wilson and Schooler’s jam test, (discussed in section 1.3 and diagramed in Figure 3.1). In the jam study, *Consumer Reports* magazine had seven taste testers who were trained sensory specialists rank forty-four jams in order from worst to best. The control group was asked to first perform a filler task where they filled out a survey of the reasons why they chose their major. They were then asked to perform the actual task of the experiment, where they ranked five jams by their order of preference. The reasons analysis subjects, the second group, were asked to perform the same task of ranking the same five jams, but were also instructed to “analyze why you feel the way you do about each” jam (Wilson & Schooler 183).
Figure 3.1:
1. A corpus of 45 jams is given to a group of taste-testing experts, who judge each jam based on 16 sensory characteristics. These results are averaged and then used to compute the ranking of each jam.
2. The control group first performs a non-related filler task, filling out a survey about why they chose their major. They are then given five of the 45 jams (1\textsuperscript{st}, 11\textsuperscript{th}, 24\textsuperscript{th}, 32\textsuperscript{nd}, and 44\textsuperscript{th}) and then asked to make decisions about the corpus of input. With a mean correlation between these results and those provided by the experts of 55\%, these results are considered meaningfully correlated to those of the experts. 
3. The second group of subjects is assigned to have the reasons analysis condition. They receive the same corpus of input, but are instructed to write down, if they wish, their reasons for choosing each jam. With a mean correlation between these results and those provided by the experts of 11\%, these results are significantly lower than those of the control group, indicating that the act of introspection may be the cause for the poorer performance.

In designing our study, we will base our design in part on that of Wilson and Schooler’s jam study. Our study should have a similar expert baseline against which we can compare the results of our experimental groups. We will also be sure to have the control group perform a filler task, so as to make the experimental groups performing their activities for the approximate same amount of time. After performing this task, the control group will carry out the actual security-related task. Finally, we will have the second group perform some sort of introspection task, as was done in the jam study, before executing the same security-related task.
Figure 3.2:
1. A corpus of items are given to two Subject Matter Experts (SMEs), who judge the input and make a decision as to whether or not to trust each item of input.
2. The first group will be the control group. This group will first perform a non-related filler task, and then be asked to make decisions about the corpus of input.
3. The second group will be an experimental group. They will receive the same corpus of input, but be asked to articulate their reasons why they are choosing to trust each input or not.
4. The fourth group will also be an experimental group. They will be asked to configure the settings for a security policy, and then make decisions about the corpus of input.

Figure 3.2 portrays the model around which we would like to form our study. We will have two Subject Matter Experts (SMEs) who are considered to be experts within the field of computer security. These experts will perform the security task, and the mean of their results will form our baseline for comparison. Group A will represent our control group, which will need to perform a non-related filler task in order to keep the time consistent with Group B. Our Group B will most likely be divided into two groups. Group B1 will fill out a survey that causes introspection about their security policies. Group B2 will have to configure some security settings using a security policy interface.
Afterwards, both groups will be asked to evaluate the corpus of items that the experts and control group have evaluated. Our hypothesis is that both Groups B1 and B2 will perform at a worse level than Group A, who we believe will perform at a level that correlates relatively well with our SMEs.

### 3.3 Web Browser User Studies

In considering potential user studies, each candidate will be considered against the requirements stated in Section 3.1 and the model discussed in Section 3.2. We are first going to consider user studies that test web browser security policies. One potential study in this realm is to ask users to adjust many security settings in a web browser, and then to see whether their policy results in trusting dangerous websites. The dangerous
phishing websites, and could make use of features of a web browser, such as lock icons or other indicators given by the web browser to signify safe websites. Such a study could certainly be conducted in the span of a month. This study would also be easily administrable from Dartmouth, as the student body would provide a sufficient number of participants. Every Dartmouth student is required to own a computer and use the Internet for their courses, so no training would be required with respect to how to use the web browser. Training of how to use the browser’s security policy, however, would be required.

With this particular example, there are several possible studies we could choose to make of it. One idea is to mimic Wilson and Schooler’s jam study (discussed in Chapter 1). To do this, we would have the control group simply create their security policy, while the test group would be asked to create a security policy as well as to articulate or write down the reasons why they were choosing each of the settings that they are. If the test group performed worse than the control group, this would give evidence that making security policies is a locked-room activity, which would imply that this fact should be taken into consideration in future designs for policy interfaces.

Another potential study is one where the control group is informed only of the necessary information about how to set the settings in their browser and what each of the settings mean. The test group, however, would be given a plethora of information about these settings, including reasons why they might choose to turn each setting on or off, information about the risks of not setting something in a particular way, as well as advice about which settings are the safest. If the control group performed better in this study, it would support the idea that there is a limit to how much information a human can pay
attention to at once. This would suggest that having large, complex policy interfaces with a multitude of different settings and ways that they can be adjusted is not an effective way of allowing users to manage their security policies.

A different study that might yield interesting results would be to show the test subjects a series of web pages and ask whether or not they would choose to trust this website. After completing this task, users would be asked to create their security policy that would trust the websites they trust, and not trust any of the sites they chose not to trust. If the policies that were created fail to match the users’ mental policies, then this would be a very strong indicator that users are unable to create the policies that they actually wish to make. Results of this study also have the potential to prove that users actually make very intelligent policies in their heads, even though these are not reflected in the policies that they actually set.

Each of these studies satisfies the requirement of having an oracle because there will be trustworthy websites and non-trustworthy websites based on how we create them. Therefore, if a user trusts a website that has been designated untrustworthy, then it can be said that they have made a wrong decision. While the studies do not inherently demand motivation of the user, paying the participants can enforce this. Those who create more successful security policies can be rewarded by being paid more for their participation in the study than those who create less successful policies. If conducted properly, all of these studies are ethical.
3.4 File Permissions User Studies

Now we will consider user studies that test file permission security policies. One idea for a file permissions study is to put the test participant into a simulated scenario where a shared network is necessary. An example may be to mock up a network like that of the registrar’s office at Dartmouth College. In this network, the registrar needs to be able to read every file so as to compile the cumulative grades for each student and present this final transcript to each student upon request. Professors must be able to read and write to files that they create, but should not be able to read any of the transcript files for any students. The registrar must be able to read these files created by professors, but should not be allowed to write to them. Finally, students should be allowed to read the transcript files produced by the registrar for themselves only (not for any other student), but should not be allowed to write to any file. Students need not have read access to the files created by the professors.
With this intricate web of file permissions, one mistake could lead to disaster. The participant of the user study would be asked to set the file permissions to match all of these settings. Such a study could certainly be completed within a month. This study could be very well conducted from the Dartmouth campus, using students as the test subjects. This study could also be easily kept to less than two hours. There would also be a very clear oracle baseline. As with the web browser studies, monetary compensation based on performance in the user study could serve to motivate participants to perform at their best. And if performed correctly, this story will surely be ethical.

One problem with this study, however, is the training required. The average person does not know how file permissions work, or even realize that they exist. This is because most people do not participate in shared file networks except for in a work
environment. The concept is not terribly complex, so I am confident that users are capable of understanding how the system works. But, confusion about doing this for the first time may be the cause for poor performance. What we want to test for, specifically, is that the user is unable to turn their mental policy into an actual policy because of the way the interface forces them to do so. Poor results from this experiment would not conclusively show this, so a different study may be better for our purposes.

Another idea for a file permission study is one where the user is using a peer-to-peer (P2P) program for downloading files from a shared network of users, such as Limewire or BearShare. Users could be asked to safely download certain files, while making sure that their settings do not allow other users to access the files on their computer.

Alternatively, users could be placed in a simulation of a financial institution. In this scenario, a basic model of the company would already be laid out for the user, with established permission settings already in place. As time elapses, however, the user could be asked to modify the file permissions based on employee movement within the company, the completion of projects and the creation of new projects, the removal of employees from the system due to being fired or leaving the company after a consulting period has ended, or the addition of new employees to the system who need access to particular things to do their new jobs. The map of permissions could easily become complicated very quickly, which might result in the test subject’s inability to set the permissions in the way they think they are. There are many difficulties associated with assigning employees access to the resources they need, given that they may hold multiple titles that require them to have access to many different types of files. As employees are
promoted, they may need their access revoked from resources they once were allowed to use. For example, someone who switches roles within the payroll department, from being the person who issues checks to being the person who signs them, must necessarily have their permissions to do these tasks reversed, otherwise a conflict of permissions would arise. Such a study could very powerfully demonstrate the challenges associated with setting resource permissions in the way that we intend. It may be difficult to produce an elegant simulation with the given time restrictions for our study. But if time were not an issue, this would likely be a very viable candidate among the others for potential user studies to conduct.

Another interesting study would be to investigate iTunes and the way this program enables music sharing over a local network. Ideally one could search for vulnerabilities in this service. For example, one might discover that enabling music sharing gives other users access to more than just the music files on your computer. Or perhaps it is possible for a malicious user to create a network that can be connected to which actually attacks users who connect to their computer. Other unforeseen loopholes might be discovered as well. While this examination might turn up some interesting results, it is not in line with the model we are trying to mimic. As a result, we will not conduct such an investigation.

A final idea for a user study is to simulate the access privileges within a hospital of doctors to patient medical records. Obviously doctors need access to their own patient’s records, but nobody else should be allowed to view this private information. In many emergency rooms, doctors are required to enter a personal user ID to access drugs they wish to give their patients. This system is supposed to keep track of which doctors
are giving out which medication, flagging any abnormal withdrawal patterns of particular
doctors. Test subjects could be asked to create the policy that will lock down the
medicine cabinet, or to alert other individuals in charge of monitoring of questionable
behavior. Test scenarios could be run against the final policy to demonstrate where it fails
and succeeds. This may be a difficult challenge to ask college students to perform,
however. Getting the number of doctors needed for substantial results may also be
undoable given our issues concerning time and administration of the experiment from
Dartmouth College. Also, creating such a simulation may be too much to do within the
window of time we have available to conduct this study. Given our restraints, the
medical study is not feasible.

3.5 Email User Studies

The last category of studies to consider are the ones that look into the use of email
security policies. One study could put the subjects into a simulated scenario that requires
them to determine the authenticity of the emails they are receiving. For example, we
could use our registrar example again. The participant could be a worker in the Office of
the Registrar at Dartmouth College, and receive emails asking them to perform various
tasks, such as issue transcripts requested by students, record grades sent in by professors,
or assign a student an incomplete for a course as requested by their class dean. Some of
these emails can be considered trustworthy, while others can be from students who have
hacked into the system to try to accomplish a mischievous goal. The test subject can be
shown this series of emails and asked to perform tasks based on whether or not they trust
the emails coming in. Poor performance would show that users do not do a good job of
recognizing the signs that can indicate fraudulent emails. While these results might prove useful in their own right, this is not quite the type of problem we are attempting to model.

One way to adjust this scenario to make it fit our model is to have the user adjust a series of security settings that should automatically determine the trustworthiness of incoming emails. The biggest issue with this study, however, is that there are no known email clients that have security interfaces that are adjustable to this degree. One would need to be developed for the purposes of this study, which is infeasible for us due to time constraints. However, the results of such a study could show the difficulty that humans have in getting a policy interface to reflect the mental policy that they have in mind.
Chapter 4

The User Study

4.1 Subjects and Recruitment

The subjects who participated in this study consisted of 100 undergraduate students—56 women and 44 men. Students were composed of various majors and class years. The test subjects were divided evenly betwixt the control and experimental groups, placing 50 in each group. Subjects were recruited by an email (see Appendix A1) that was sent out to the entire Dartmouth campus, advertising a behavioral experiment related to Facebook that needed research participants. Subjects volunteered to participate in the half-hour study in exchange for $15. The only requirement that was demanded of each subject was that he or she currently has a Facebook account. This study was approved by the Committee for the Protection of Human Subjects (CPHS), the Institutional Review Board (IRB) at Dartmouth College.
4.2 Part I – The Questionnaire

The study was divided into two parts. The first part required five to ten minutes to complete a questionnaire. We created two questionnaires—one for the control group and one for the experimental group. (The significance of the two questionnaires will be discussed later in Section 4.4.) The control group filled out a questionnaire that asked questions related to how they picked their major in college. The content of this questionnaire was unimportant, and was picked simply because each test subject was a college student at Dartmouth College and would find these questions relevant to his or her life. The questionnaire was designed to be twenty-five questions long, consisting of a variety of yes-or-no questions, questions asking the user to pick a value on a scale from one to ten, and questions about when in their college career certain decisions were made. Several of the questions related to one’s happiness with their major, or whether happiness ought to even be a factor in one’s decision of what to major in during college.

The experimental group had a completely different questionnaire to fill out during the first phase of the study. This questionnaire asked questions about the subject’s configuration of privacy settings on his actual Facebook account. Most of these questions asked the subject to assume that Facebook had an interface that allowed him to easily configure his security settings in any way that he wants, and then asked how the various settings would be configured. Some additional questions also asked the subject if she had anything on her Facebook account that she would not want various people (an employer, a professor, a parent, etc.) to see. This questionnaire was twenty-seven questions long, and was estimated to take the approximate same amount of time as the questionnaire that the control group was asked to fill out.
4.3 Part II - InnerCircle

The second portion of the experiment incorporated a fake social networking site that strongly resembled the structure of Facebook. The decision to not use Facebook was made for a few reasons. To present users with a series of Facebook profiles seemed to pose the problem that users would not be able to get a good sense for how well they know each person that was shown to them. To understand how well you know someone, we decided it was important to understand the context in which you met them or have interacted with them since you knew them, as well as how long you have known them. This information could not be derived from a Facebook profile alone. This social networking site we designed to use instead was called InnerCircle and contained many components that were identical to Facebook, including a Profile Picture, the idea of Networks, Photo Albums, and Groups. While most of the information was presented in a way very similar to how one would see it on a Facebook profile, there were a few new concepts on these profile pages, which we created to give the user a sense of actually knowing and being friends with these people in real life.

Figure 4.1 depicts one of the profiles used in the study. One important difference found in each InnerCircle profile that would not be on Facebook is a section of information about how the test subject met the person in the profile. Michael’s profile in Figure 4.1 shows that there is a “How do you know Michael?” question, which has an answer that the test subject is said to have filled out when they added this person as a friend in their InnerCircle. This question was included to establish the type of relationship
the test subject has with the person in the profile they are viewing. Presumably one’s privacy settings would be different based on this information. For example, one might not want their boss from their job to view their photos, but they might want to let their roommate see their photos. Another question in this section that we added to InnerCircle was “When did you and [Person X] meet?” This information was included to give the subject a sense of how long they have been friends with the person, in case that has an impact on how much information they wish to share with a given InnerCircle friend.
There is one more section of information that is unique to InnerCircle and is worth noting. This box provides information that shows how much the subject is connected to the person in the profile. Subjects were told that InnerCircle generates this data, which includes how much their friend circles overlap, that is how many friends do they have in common, how many photos both of these people are tagged in together, when was the last time the subject sent or received a message from this user, and how close geographically the subject is to this user, (based on the Current Location listed on their profile). The test subject participating in the experiment is told that this information is generated by the InnerCircle website, as opposed to being provided by the user.

Lastly, there is an “Interesting Fact” included in each profile about the person portrayed in the profile. This was included simply to give the people in the profiles more of a unique identity, with the hope that the test subjects would be able to further suspend their disbelief of not actually knowing these people in real life. Our hope was that the more of a unique relationship the subjects feel that they have with these people, the more accurate their privacy decisions will be to what they would do in real life on Facebook.

<table>
<thead>
<tr>
<th>Would you allow Amanda to view . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Yes</td>
</tr>
<tr>
<td>□ Yes</td>
</tr>
<tr>
<td>□ Yes</td>
</tr>
<tr>
<td>□ Yes</td>
</tr>
<tr>
<td>□ Yes</td>
</tr>
<tr>
<td>□ Yes</td>
</tr>
<tr>
<td>□ Yes</td>
</tr>
</tbody>
</table>

Figure 4.2 These seven questions were asked of about each profile that was shown to the test subjects during the experiment.
The test subjects were shown twenty InnerCircle profiles. (For a complete set of images of all profiles that were shown during this experiment, in the order that they were shown, see Appendices P1 through P20.) The profiles were shown in a pre-generated random order. Users were asked the same seven questions (shown in Figure 4.2) about each profile. These questions were selected to directly mimic the seven key areas of Facebook to which users are allowed to configure access by other Facebook users. On Facebook, these settings are made more broadly. For example, in the Privacy Settings area of Facebook, one can set their Basic Info to be viewable by “Everyone,” “My Networks and Friends,” people in my primary network and Friends, “Friends of Friends,” or a customized variation of this. We designed InnerCircle to be more explicit in these decisions, however, by requiring the user to make these choices with respect to every profile.

This part of the experiment took users anywhere from fifteen to twenty-five minutes to complete. Finally, upon completing the InnerCircle profile evaluations, the user was asked to fill out a post-test feedback questionnaire (Appendices A4 and A5).

4.4 Experimental Hypothesis

As was previously mentioned, the answers that either group gave on their questionnaire were unimportant to us; it was the act of filling out the questionnaire that was meaningful. The major questionnaire that was given to the control group was merely a filler questionnaire that would require the same amount of time as the Facebook questionnaire, as well as acclimate the control users to the experimental environment.
The real purpose behind having a questionnaire, however, was to have the experimental group “introspect” upon their own Facebook privacy settings. Put another way, we believed that the act of thinking about one’s privacy policies (the act of introspection) was significant, possibly enough to transform the decisions that were made during the second portion of the experiment. Thus, our experimental hypothesis was that introspection inhibits intuition. We expected the act of introspecting upon one’s own Facebook security policies to cause the experimental group to lose track of their own intuitive security policy that they would have wished their InnerCircle privacy policies to express.

We predicted that if any loss of intuition were to manifest itself in our results, it would cause the control group’s InnerCircle decisions to be more clustered, or consistent, than those of the introspective group. This is to say that there was not so much of a concept of there being “correct” answers, but instead that the users in the control group would all make similar selections when configuring their InnerCircle privacy policies. The experimental group’s answers were expected to have a higher standard of deviation, varying greatly not only from the control group’s answers but from each other’s answers as well.
Chapter 5

Results of the User Study

5.1 Original Hypothesis

As was discussed in Section 4.4, our experimental hypothesis was that introspection inhibits intuition. It was our belief that the act of introspecting upon one’s own Facebook security policies would cause the experimental group to lose track of their own intuitive security policy that they would have wished their InnerCircle privacy policies to express. There are several ways that this loss of intuition might manifest itself in our results. One option is that the control group’s InnerCircle decisions would be more clustered, or consistent, than those of the introspective group. By contrast, this would mean that the experimental group’s answers would be expected to have a higher standard of deviation, varying greatly not only from the control group’s answers but from each other’s answers as well.
Another way that a loss of intuition might manifest itself would be if a dichotomy were to form between the two groups. It might be the case that both groups made consistent decisions within the group, resulting in comparable standards of deviation, but that the decisions would differ between the two groups. For example, perhaps there would be a subset of profiles to which the control group restricted access to all of their sensitive data, but to whom the introspective group would have a more open policy regarding their private information.

Alternatively, we considered the possibility that the introspective group might simply appear to be more confused than the control group. This is not to say that there are “right” or “wrong” decisions, but clearly some decisions should follow based on others. For example, it would not make sense for one to restrict access to his photos from a teammate from the track team, but to allow access to these photos to someone who he had never met before. Another confusing decision would be for a subject to allow her boss from her internship last summer to view her Personal Information, but to disallow her best friend since preschool from seeing this same information.

5.2 Analysis of Results

From the data gathered during our experiment, we are able to conclude that introspection does indeed inhibit one’s intuition. One of the ways this was demonstrated was simply by the number of yes-answers that were given during the InnerCircle portion of the experiment. The number of yes-answers given can be equivocated to the openness of one’s privacy policy, since a “yes” means that the user allowed their information to be
shared, while a “no” means that they would not share a piece of personal information with the given profile. The results of the user study showed that the mean number of yes-answers given by the control group was 86.6, while the mean for the introspective group was 98.56. It is possible that this difference is not statistically significant, so to determine whether it was, we ran an ANOVA F-test on the experimental data. The result of this F-test was an F of 6.57, which means that the difference in average total yes-answer counts is indeed statistically significant. From this we were able to conclude that the introspective group was much more willing to share their information than the control group.

The next data set we examined was that which describes how the two groups shared their information according to the type of question they were asked. In the study there were seven types of information one could either share or refuse to share: Basic Information (Sex, Birthday, Hometown, Relationship Status, Political Views, and Religious Views), Personal Information (Interests, Favorite Music, Favorite Movies, Favorite Books, Favorite Quotes, and an About Me section), Email Address (a non-

<table>
<thead>
<tr>
<th>Category</th>
<th>Mean</th>
<th>Standard Deviation</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Info</td>
<td>88.61</td>
<td>10.07</td>
<td>5</td>
<td>95</td>
</tr>
<tr>
<td>Personal Info</td>
<td>76.60</td>
<td>17.80</td>
<td>25</td>
<td>95</td>
</tr>
<tr>
<td>Email</td>
<td>77.42</td>
<td>18.48</td>
<td>3</td>
<td>95</td>
</tr>
<tr>
<td>Phone</td>
<td>48.92</td>
<td>27.52</td>
<td>0</td>
<td>95</td>
</tr>
<tr>
<td>Address</td>
<td>48.00</td>
<td>29.39</td>
<td>0</td>
<td>95</td>
</tr>
<tr>
<td>Photos</td>
<td>57.45</td>
<td>22.64</td>
<td>0</td>
<td>95</td>
</tr>
<tr>
<td>Videos</td>
<td>54.44</td>
<td>25.45</td>
<td>0</td>
<td>95</td>
</tr>
</tbody>
</table>

**Figure 5.1** This table displays the mean percentage of all 100 users (averaged over all twenty profiles) who granted access to each of the seven types of information in the experiment. The standard deviation of these averages is also shown, as well as the minimum and maximum percentage of yes-answers for each category that were given.
school email), Phone Number, Current Mailing Address, Photos that tagged the user in them, and Videos that tagged the user. As can be seen from Figure 5.1, the test subjects on the whole were most protective of their phone numbers and mailing addresses, followed by caution when giving out their photos and videos.

<table>
<thead>
<tr>
<th></th>
<th>% of Average (Control)</th>
<th>% of Average (Introspective)</th>
<th>Standard Deviation (Control)</th>
<th>Standard Deviation (Introspective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Info</td>
<td>88.37</td>
<td>88.85</td>
<td>10.23</td>
<td>10.01</td>
</tr>
<tr>
<td>Personal Info</td>
<td>73.88</td>
<td>79.38</td>
<td>20.06</td>
<td>14.86</td>
</tr>
<tr>
<td>Email</td>
<td>78.33</td>
<td>76.53</td>
<td>19.11</td>
<td>18.00</td>
</tr>
<tr>
<td>Phone</td>
<td>41.86</td>
<td>55.82</td>
<td>27.22</td>
<td>26.29</td>
</tr>
<tr>
<td>Address</td>
<td>43.96</td>
<td>52.13</td>
<td>29.96</td>
<td>28.53</td>
</tr>
<tr>
<td>Photos</td>
<td>51.00</td>
<td>63.88</td>
<td>25.90</td>
<td>16.75</td>
</tr>
<tr>
<td>Videos</td>
<td>47.55</td>
<td>61.33</td>
<td>28.40</td>
<td>20.15</td>
</tr>
</tbody>
</table>

**Figure 5.2** The first two columns of this table display the mean percentage of users (averaged over all twenty profiles) who granted access to each of the seven types of information in the experiment. The next two columns show the standard deviation corresponding to these averages.

Figure 5.2 displays the mean number of yes-answers given in each of the seven question-type categories, this time splitting up the means by control group and introspective group. In the categories of Basic Info and Email, the difference between the averages of the control group and the introspective group were clearly negligible. However, the discrepancies were greater for the remaining five categories, possibly showing a significant difference in behavior between the two groups.

To determine whether or not these discrepancies were meaningful, we had the choice of running an unpaired T-test or an F-test on the means. T-tests are good for small populations of approximately 20 or less, but because we had 50 users in each category, we felt confident in using the F-Test. After running ANOVA F-tests on each of these pairs of averages (Figure 5.3), we were able to determine that the differences between Personal Info (F=2.34) and Address (F=1.85) were not statistically significant, but that
The first column shows the difference between the averages for the control and introspective group that were displayed in Figure 5.2. The second column shows the differences between the standard deviations presented in Figure 5.2. The third column shows the results of an ANOVA F-Test on these averages.

<table>
<thead>
<tr>
<th>Difference Between Averages</th>
<th>Difference Between Standard Deviations</th>
<th>F-Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Info</td>
<td>0.48</td>
<td>0.22</td>
</tr>
<tr>
<td>Personal Info</td>
<td>5.50</td>
<td>5.20</td>
</tr>
<tr>
<td>Email</td>
<td>1.80</td>
<td>1.11</td>
</tr>
<tr>
<td>Phone</td>
<td>13.96</td>
<td>0.93</td>
</tr>
<tr>
<td>Address</td>
<td>8.17</td>
<td>1.43</td>
</tr>
<tr>
<td>Photos</td>
<td>12.88</td>
<td>9.15</td>
</tr>
<tr>
<td>Videos</td>
<td>13.78</td>
<td>8.25</td>
</tr>
</tbody>
</table>

Figure 5.3 The first column shows the difference between the averages for the control and introspective group that were displayed in Figure 5.2. The second column shows the differences between the standard deviations presented in Figure 5.2. The third column shows the results of an ANOVA F-Test on these averages.

The difference of means of the Phone (F=6.58), Photos (F=8.51), and Videos (F=7.67) were all statistically meaningful. This data supports the conclusion that the introspective group was not only more willing to share their information than the control group, but that the information they shared more of was their most sensitive information. Hence, one of our experimental hypotheses, that there might be a dichotomy between the choices of the control and introspective groups, was proven to be the case.

Figures 5.4 and 5.5 chart out the introspective group’s willingness to share the three sensitive data types that the control group was not as willing to share—Phone Number, Photos, and Videos. Figure 5.5 orders these by openness to each profile, showing a scale of how trusting the introspective users were for each profile. This reveals that in some instances the introspective users seemed to make “wrong” decisions. Profile 5 (Appendix P5) was tied for being one of the most trusted users with the three sensitive types of data, but Profile 5 represented Jake Mehrens—someone you had met.
Figure 5.4 This chart shows the introspective group’s willingness to share the three sensitive types of data, laid out per profile. Here d represents Phone Number, f represents Photos, and g represents Videos.

Figure 5.5 This chart orders the data from Figure 5.4, ordering the profiles by the amount of trust the introspective group gave them with the three types of sensitive data, (Phone Number, Photos, and Videos).
only once at a weekly dance club at Dartmouth College. Somehow Jake was trusted the most after only meeting once. Two other profiles represented acquaintances you had also only met once. Andrew P. (Profile 10) was someone you met at a party who seemed funny, while Phil (Profile 8) was someone you met at a party who seemed sketchy. Both of these one-time acquaintances were in the middle of the range of sensitive data.

Confusingly, however, Maddie (Profile 15) was given the approximate same access to this sensitive data as was sketchy Phil, and yet she was one of your former teammates on the track team during your first two years of college. Another perplexing case was that of Darcy (Profile 13) and Colleen (Profile 16). Colleen was someone you friended simply because she shares your same favorite band of Queen. Darcy was someone you friended simply because you share the same top 5 movies. Darcy, however, is ranked significantly higher than Colleen, who received the lowest ranking. This is likely due to the fact that Darcy is a Dartmouth student, while Colleen is a student at Lehigh University. It is not surprising that subjects would be more willing to share with a stranger within their network than with a stranger outside of their school’s network, however the disparity between the quantities of information shared with Darcy and with Colleen is a bit surprising.

Speaking of Colleen brings to mind an anecdote. While harvesting the data during the study, I had a research assistant help me enter the data into a spreadsheet for all the users. We quickly noticed that Colleen was not very well received. We notice that no one had ever given Colleen his or her phone number in the study. Partway through the study, my assistant and I were shocked to discover the first user to share their phone number with Colleen. Soon it became a running joke between us to judge people
based on whether or not they would share their phone number with Colleen. It was not
till later that we learned that two of our very good friends who had participated in the
study had been the only two users at that point to share their phone numbers with
Colleen. Though there are no actual “right” or “wrong” answers, clearly there are
decisions that are generally assumed to be wise or unwise.

The final way we chose to examine the data was to again compare the control
group with the experimental group in terms of the average number of yes-answers given.
This time, however, we looked at these averages per profile, rather than per question
type. Figure 5.6 shows the mean number of yes-answers given for each of the twenty
profiles that were shown to test subjects during the study.

<table>
<thead>
<tr>
<th></th>
<th>% of Average</th>
<th>% of Average</th>
<th>Standard Deviation</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Control)</td>
<td>(Introspective)</td>
<td>(Control)</td>
<td>(Introspective)</td>
</tr>
<tr>
<td>1-Wade</td>
<td>68.80</td>
<td>83.38</td>
<td>28.22</td>
<td>19.64</td>
</tr>
<tr>
<td>2-Chatham</td>
<td>50.29</td>
<td>61.51</td>
<td>32.17</td>
<td>33.66</td>
</tr>
<tr>
<td>3-Arthur</td>
<td>81.05</td>
<td>92.71</td>
<td>23.58</td>
<td>16.27</td>
</tr>
<tr>
<td>4-Danny</td>
<td>62.10</td>
<td>71.73</td>
<td>22.30</td>
<td>23.48</td>
</tr>
<tr>
<td>5-Jake</td>
<td>58.29</td>
<td>72.01</td>
<td>30.39</td>
<td>28.71</td>
</tr>
<tr>
<td>6-Andrew V.</td>
<td>86.00</td>
<td>95.43</td>
<td>18.14</td>
<td>10.18</td>
</tr>
<tr>
<td>7-Amanda</td>
<td>82.29</td>
<td>88.63</td>
<td>21.32</td>
<td>15.70</td>
</tr>
<tr>
<td>8-Phil</td>
<td>47.71</td>
<td>55.43</td>
<td>29.80</td>
<td>34.23</td>
</tr>
<tr>
<td>9-Beth</td>
<td>56.57</td>
<td>62.10</td>
<td>28.12</td>
<td>33.45</td>
</tr>
<tr>
<td>10-Andrew P.</td>
<td>68.86</td>
<td>77.71</td>
<td>25.27</td>
<td>24.69</td>
</tr>
<tr>
<td>11-Samantha</td>
<td>81.71</td>
<td>94.86</td>
<td>23.98</td>
<td>11.46</td>
</tr>
<tr>
<td>12-Michael</td>
<td>47.43</td>
<td>53.06</td>
<td>23.35</td>
<td>26.57</td>
</tr>
<tr>
<td>13-Darcy</td>
<td>40.29</td>
<td>47.14</td>
<td>31.58</td>
<td>37.21</td>
</tr>
<tr>
<td>14-Megan</td>
<td>94.86</td>
<td>98.00</td>
<td>12.83</td>
<td>7.08</td>
</tr>
<tr>
<td>15-Maddie</td>
<td>81.43</td>
<td>87.43</td>
<td>20.05</td>
<td>18.62</td>
</tr>
<tr>
<td>16-Colleen</td>
<td>29.74</td>
<td>24.86</td>
<td>29.42</td>
<td>30.52</td>
</tr>
<tr>
<td>17-Peggy</td>
<td>54.29</td>
<td>66.29</td>
<td>25.98</td>
<td>25.29</td>
</tr>
<tr>
<td>18-Cam</td>
<td>50.00</td>
<td>56.27</td>
<td>31.25</td>
<td>32.79</td>
</tr>
<tr>
<td>19-Kate</td>
<td>61.43</td>
<td>75.71</td>
<td>28.90</td>
<td>25.04</td>
</tr>
<tr>
<td>20-Maddie</td>
<td>65.71</td>
<td>78.00</td>
<td>28.86</td>
<td>23.66</td>
</tr>
</tbody>
</table>

Figure 5.6 The first two columns of this table display the mean number of users (averaged over
the seven different types of questions) who granted access to each of the twenty profiles in the
experiment. The next two columns show the standard deviation corresponding to these averages.
Again there were a number of discrepancies between the control and introspective group for averages with respect to particular profiles. After again running an ANOVA F-test on the pairs of averages for each profile (Figure 5.7), we found that the discrepancies exhibited between the averages for profiles 1, 2, 3, 4, 5, 6, 11, 17, 19, and 20 were all statistically significant. If it were not clear enough before, this provides even more evidence to further our claim that there was a clear dichotomy between the way that the control and introspective groups performed.

<table>
<thead>
<tr>
<th></th>
<th>Difference Between Averages</th>
<th>Difference Between Standard Deviations</th>
<th>F-Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Wade</td>
<td>14.58</td>
<td>8.58</td>
<td>8.81</td>
</tr>
<tr>
<td>2-Chathum</td>
<td>11.22</td>
<td>1.49</td>
<td>2.88</td>
</tr>
<tr>
<td>3-Arthur</td>
<td>11.66</td>
<td>7.31</td>
<td>8.12</td>
</tr>
<tr>
<td>4-Danny</td>
<td>9.63</td>
<td>1.18</td>
<td>4.29</td>
</tr>
<tr>
<td>5-Jake</td>
<td>13.72</td>
<td>1.68</td>
<td>5.33</td>
</tr>
<tr>
<td>6-Andrew V.</td>
<td>9.43</td>
<td>7.96</td>
<td>10.28</td>
</tr>
<tr>
<td>7-Amanda</td>
<td>6.34</td>
<td>5.62</td>
<td>2.83</td>
</tr>
<tr>
<td>8-Phil</td>
<td>7.72</td>
<td>4.43</td>
<td>1.44</td>
</tr>
<tr>
<td>9-Beth</td>
<td>5.53</td>
<td>5.33</td>
<td>0.79</td>
</tr>
<tr>
<td>10-Andrew P.</td>
<td>8.85</td>
<td>0.58</td>
<td>3.14</td>
</tr>
<tr>
<td>11-Samantha</td>
<td>13.15</td>
<td>12.52</td>
<td>12.23</td>
</tr>
<tr>
<td>12-Michael</td>
<td>5.63</td>
<td>3.22</td>
<td>1.26</td>
</tr>
<tr>
<td>13-Darcy</td>
<td>6.85</td>
<td>5.63</td>
<td>0.99</td>
</tr>
<tr>
<td>14-Megan</td>
<td>3.14</td>
<td>5.75</td>
<td>2.30</td>
</tr>
<tr>
<td>15-Maddie</td>
<td>6.00</td>
<td>1.43</td>
<td>2.40</td>
</tr>
<tr>
<td>16-Colleen</td>
<td>4.88</td>
<td>1.10</td>
<td>0.66</td>
</tr>
<tr>
<td>17-Peggy</td>
<td>12.00</td>
<td>0.69</td>
<td>5.48</td>
</tr>
<tr>
<td>18-Cam</td>
<td>6.27</td>
<td>1.54</td>
<td>0.95</td>
</tr>
<tr>
<td>19-Kate</td>
<td>14.28</td>
<td>3.86</td>
<td>6.98</td>
</tr>
<tr>
<td>20-Maddie</td>
<td>12.29</td>
<td>5.20</td>
<td>5.42</td>
</tr>
</tbody>
</table>

**Figure 5.7** The first column shows the difference between the averages for the control and introspective group that were displayed in Figure 5.6. The second column shows the differences between the standard deviations presented in Figure 5.6. The third column shows the results of an ANOVA F-Test on these averages.
One type of behavior was clear; the introspective users appeared to only have two types of buckets in which to place each profile. Many introspective users even explained this, saying that if they had friended someone then they felt weird denying them access to any of their personal information, (see post-test questionnaire comments in Section 5.4). The control users seemed to exhibit a much wider gradation, however, when it came to configuring the access to their personal information by other users. It would seem that the introspection caused the users to lose their ability to figure out why to deny.

5.3 Possible Explanations

As was shown, there is much evidence to support the claims that the introspective group answered questions significantly differently than the control group. Not only was the introspective group more open on the whole, but also they were more open with their most sensitive data. Several possible explanations for this behavior exist. One idea is that when a person considers the many instances for which they might wish to deny or allow access to information, it leaves her unable to come up with reasons for having had rules in the first place. This might cause her to drop any rules she previously held, leaving her to default to allowing access to their private information unless she is given a “good” reason to deny someone access. This would certainly explain why many of the introspective users shared significantly more information than the control subjects.

Similarly, another option is that reflecting on the reasons why one should grant or deny access to their personal information leads the subjects to believe that they must have a really good reason why they are denying a person access. Without concrete reasons to
back them up, perhaps the user is unable to feel comfortable trusting his intuitions, and thereby resorts to the default of granting access to everyone.

One possible explanation that we have considered was that we were simply priming the introspective users to be thinking about their privacy policies, which led them to behave in the way that they did. Perhaps the way we phrased the questions, by saying “Would you allow [Person X] to view…” was done in a biased manner. Had we phrased it to say “Would you deny [Person X] access to…” we may have gotten some very different answers. To test the effects of this, perhaps future work can be done to alter this aspect of the study.

Another effect to take into consideration is the ratio of men to women. It is possible that the control group simply had a large concentration of the women who participated in the study. Were this the case, then the effects might be explained by a societal factor that causes women to be more protective of their private data than men. In his talk at the 2003 Workshop on Human-Computer Interaction and Security Systems, Paul Dourish of UC Irvine observed that his user studied showed that female users tended to associate computer privacy leaks—such as random users being able to figure out that user X was in a terminal room in the library alone late at night—with potential threats to their physical person. This suggests a hypothesis that men are more likely to share sensitive data than women are. This is not likely to be the source of any of the effects we have noticed on the introspection group, however, as there were 28 females and 22 males in both the control group and the experimental group. The gender was fairly balanced within each group, and the two groups had identical gender balances either way. For
these reasons, it is very doubtful that the effects observed in the study were produced simply as the result of any gender balance issues.

### 5.4 Future Work

There are several ways of explaining the effects that were produced by this study. For this reason, it would behoove the research community to continue pursuing this direction. Reenacting this experiment with slight alterations might lead toward a more concrete explanation of the effects of introspection on one’s security policies. A variation on this study might attempt to learn why the users are making the choices that they are. This could help us to understand why the introspective group believes they should be making the choices that they are, as well as the control group, and give us more insight into what is actually going on here.

As was mentioned above, another potential alteration to make to this study would be to rephrase the questions from saying “Would you allow [Person X] to view…” to say “Would you deny [Person X] access to…” instead. If this yields the same results, then that would be even more powerful. If a different outcome is reached, however, then it would suggest that our results were achieved simply because of our priming the users to think about their security settings in such a way that the subjects became more open.

Reading the post-test questionnaires that were administered during our study has helped to get an idea about what thought processes the subjects were going through. The main patterns that we noticed were that many people in the control group wanted to go back and constrain their actual Facebook settings in real life once the study was completed. Some of the introspective users felt this way as well. Perhaps slightly more
puzzling was a trend we found only in the introspective group, and not within the control group. Several users in the introspective group expressed a sentiment similar to this one: “I mostly assumed if I [InnerCircle] friended them or accepted friendship, they’re probably ok. I ended up pretty much allowing everyone to see everything because on Facebook I don’t really monitor anyone’s.” Another introspective subject said “I usually don’t friend/accept requests from people I don’t know really well so most of my ‘friends’ have access to all my profiles.” Still another subject said “If I’m not ‘friends’ with someone, I usually delete their account so I don’t have to worry about individual policy.” This could be interpreted as the user saying that they don’t even bother to use the privacy settings because they are not worth dealing with. Another user reiterated this point in saying “…normally when I friend someone on Facebook I don’t bother to change their settings in particular.” If future work were to be done, it would be good to try to inform the users that just because someone is your friend does not mean that you have to give them access to all your information. We saw this sentiment over and over again in the post-test questionnaires for the introspective group, but not even one control user made this type of remark in their post-test questionnaire.

Many of the introspective user’s responses would lead you to believe that they were being more conservative than they really were. “I think I was more private with InnerCircle by not accepting some people when I may have potentially accepted them on Facebook. But over the years I have become more private with Facebook.” In the words of another user they thought that they were “Maybe a bit more guarded than Facebook, because Facebook is more well-established.” We did not note any of the control users making these types of remarks on their post-test questionnaires.
From these post-test questionnaires came some insightful comments that are worth taking under consideration for future work as well. One introspective subject remarked that “The only thing that was unclear was whether we are already friends with them or not… for two profiles I would not have friended them but since I assumed I did then I felt weird saying “no” to everything…” Another introspective subject said “Some of the profiles said I was a ‘friend,’ but I never would have befriended them in the first place. I wasn’t sure how to interpret that.” It is worth noting that my instructions did explain that all twenty of these profiles were people you had added as a friend on InnerCircle and that you would be choosing how much information to show each of them. Perhaps these instructions need to be made more explicit; maybe with an example before the InnerCircle evaluating begins. One of the control users also remarked that “There is an emotional component to meeting someone in real life that the profile could not capture.” A couple others noted this lack of an emotional connection that was required for making these decisions. So perhaps a different way of introducing these people would be more effective.

There are many aspects of this study that are worth maintaining, however. Many users commented to me after taking the study that they wished InnerCircle existed in real life. One user told me that InnerCircle resembled the old Facebook—a cleaner and simpler version of the current site which is in general preferred over the current version of Facebook. One user spent about five or ten minutes speaking with me about how I ought to pursue my InnerCircle idea. They even recommended that I use the results of this study to sell my ideas for InnerCircle to Mark Zuckerberg. One user wrote in their post-test questionnaire “I wish Faccebook had the option to write in how you know the
person without them seeing it.” I would recommend keeping this aspect of any fake social networking site that is designed to simulate this study. Another user even went so far as to say “The ‘how we met’ information was accurate and reflected realistically almost all the scenarios and ways I meet people and friends.” Several others from both the control and introspective groups noted that they enjoyed the “How we met” information. No one reported liking Facebook better than InnerCircle.

The last interesting fact that came from reviewing the post-test questionnaires was that many members of the control group noted that they planned to go change their Facebook settings after having gone through this experiment. Many introspective users, however, answered this question saying that they didn’t need to change their settings and would not be changing them. This is interesting because the introspective users were the ones who gave away their sensitive data more freely, while the control group were the more conservative ones.
Appendix

This appendix includes all documents that were shown to the test subjects prior to and following the user study. Also included are all the InnerCircle profiles that were viewed by the subjects during the actual experiment.
From: Stephanie.A.Trudeau@Dartmouth.EDU
Subject: Earn $15 in 30 minutes
Date: May 11, 2009 6:31:42 PM EDT

. . . by participating in my senior thesis research!

Who: Anyone with a Facebook account
What: 15-30 minute decision making study

Make a series of trust decisions about profiles on a simulated social networking site similar to Facebook.

Where: Sudikoff Laboratory
Why: Earn $15 and contribute to meaningful research!

How: Blitz me back to sign up for a time slot

Figure A1: All recruitment for the experiment was done via this email, which was sent to every undergraduate student at Dartmouth College.
DARTMOUTH COLLEGE

Usability of Security Policy Interfaces

PROJECT INFORMATION SHEET

This project is being conducted by an undergraduate student with supervision by a faculty advisor from Dartmouth College, Hanover, NH, USA. It is a study of the effectiveness of current designs for computer security policy interfaces.

Your participation is voluntary. Participation involves completing a series of tasks on a computer, as well as completing a survey. You may choose to not answer any or all questions.

The information collected will be maintained confidentially and will be anonymized by assigning a random ID number that is associated with your data. Your name will not be used in any reports developed from this research, however, with your permission the data collected from your computer session and survey may be used in reports of this research study.

Questions about this project may be directed to:

Stephanie A. Trudeau
Email: Stephanie.A.Trudeau@Dartmouth.edu
Phone: (509) 995-1041

Faculty advisor:

Sean W. Smith
Department of Computer Science
6211 Sudikoff Laboratory
Hanover, NH 03755

Email: Sean.W.Smith@Dartmouth.edu
Phone: (603) 646-1618

Figure A2: This Information Sheet was shown to all subjects before having them sign the consent form for participation in the experiment.
CONSENT TO PARTICIPATE IN RESEARCH

Dartmouth College

Study title: Usability of Security Policy Interfaces

You are being asked to participate in a research study. Your participation is voluntary.

Your decision whether or not to participate will have no effect on your academic standing or employment. You will be paid for your participation. Please ask questions if there is anything you do not understand.

This study examines decision making in a privacy related scenario. Your participation involves an experiment that is conducted on a computer and that lasts 20 - 40 minutes. In the experiment, you will sit at a computer and be presented with a series of mock profiles on a fake social networking site called InnerCircle. You will be asked to make trust decisions about each profile. At the end of the experiment you will be asked to fill out a questionnaire. Upon completion of this study, you will receive $15.

Your participation in this experiment will not expose you to any physical harm or psychological risk. Publications or other reports of this experiment will not identify you in any way. The data generated in this session will be maintained and analyzed by the investigators and, in accordance with standard academic practice, will be shared with other researchers upon request. However, the data will not identify you in any way. Your contact information will be used only to schedule the time and location for your participation in the study.

You have the right to withdraw from the experiment at any time, but if you do so you will forfeit any monetary gains.

Questions about this study may be directed to Stephanie Trudeau at (509) 995-1041 or Stephanie.A.Trudeau@Dartmouth.edu.

If you have questions, concerns, or suggestions about human research at Dartmouth, you may call the Office of the Committee for the Protection of Human Subjects at Dartmouth College (603) 646-3053 during normal business hours.

CONSENT

I have read the above information about Usability of Security Policy Interfaces and have been given an opportunity to ask questions. I understand that I am free to discontinue participation at any time if I so choose. I agree to participate in this study.

Participant’s Signature

Date

For CPHS Use Only

v. 031909

Figure A3: This consent form was signed by all test subjects prior to beginning the experiment.
Post-Test Feedback

Control User – Subject #:

1. Did all of the instructions make sense?

2. Did you understand the questions that were being asked of you?

3. What do you think was the purpose of the major questionnaire that you filled out in the beginning?

4. Was there enough information in each profile for you to make your decisions?

5. What information in each profile did you use most to make your trust decisions?

6. Did InnerCircle seem similar to Facebook? If not, why?

7. Did you feel your trust decisions on InnerCircle were similar or different than those that you have made on your Facebook account? Why?

8. Do you feel that you should make any alterations to your Facebook privacy settings after having completed this experiment?

9. Any other comments about the experiment?

Figure A4: This form was given to the control subjects upon completion of the experiment, following the evaluation of the InnerCircle profiles.
Post-Test Feedback

Introspective User – Subject #:

1. Did all of the instructions make sense?

2. Did you understand the questions that were being asked of you?

3. What do you think was the purpose of the Facebook questionnaire that you filled out in the beginning?

4. Was there enough information in each profile for you to make your decisions?

5. What information in each profile did you use most to make your trust decisions?

6. Did InnerCircle seem similar to Facebook? If not, why?

7. Did you feel your trust decisions on InnerCircle were similar or different than those that you have made on your Facebook account? Why?

8. Do you feel that you should make any alterations to your Facebook privacy settings after having completed this experiment?

9. Any other comments about the experiment?

Figure A5: This form was given to the introspection subjects upon completion of the experiment, following the evaluation of the InnerCircle profiles.
Major Selection Questionnaire

The following questions relate to your choice of major in college. Please answer all questions honestly, and to the best of your knowledge. If you have not yet chosen a major, for the purposes of this study please select what you think you would major in if you had to choose one by tomorrow.

1. What is your major? ____________________________________________

2. How long have you known this would be your major?
   ___ < 1 year
   ___ 1 – 2 years
   ___ 2 – 3 years
   ___ 3- 4 years
   ___ 5 years
   ___ > 5 years

3. On a scale of 1 to 10, how happy are you with your choice of major?
   1 2 3 4 5 6 7 8 9 10
   Not Very Happy       Extremely Happy

4. When did you take your first class in your field of study?
   ___ High School
   ___ Freshman Year (of college)
   ___ Sophomore Year
   ___ Junior Year
   ___ Senior Year

5. Before deciding to major in your field of study, had you ever taken a class in that field?
   Yes       No

6. Was your choice of major at all influenced by the other students in that major?
   Yes       No

Figure A6: This form was given to the control subjects as their first task during the experiment.
7. Was your choice of major at all influenced by the professors in that major?
   Yes  No

8. If you attended a different college, would your choice of major would be the same?
   Yes  No

9. Since matriculation, how many times have you changed your major?
   ___ Never  ___ Once  ___ Twice  ___ Three Times  ___ Four Times  ___ Five or More Times

10. About how much confidence do you have that your current major will be your actual major upon graduation?
    
    1  2  3  4  5  6  7  8  9  10
    Not Very Confident  Extremely Confident

11. How many classes in your field of study have you taken so far?
    ___ None  ___ One   ___ Two  ___ Three  ___ Four  ___ Five or More

12. Do you know what occupation you wish to seek after graduating with your major?
     Yes  No

13. Is the career you wish to seek after graduation related to your major?
    Yes  No  Don’t Know

**Figure A6 (continued):** This form was given to the control subjects as their first task during the experiment.
14. Was your decision about what subject to major in more heavily based on what career you want to pursue or on your interest in the courses related to that major?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Career Aspirations</td>
<td>Courses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

15. When do you think it is too late to change your major?

- [ ] High School
- [ ] Freshman Year (of college)
- [ ] Sophomore Year
- [ ] Junior Year
- [ ] Senior Year
- [ ] Never too late

16. If you could go back to freshman year, would you do anything differently in order to help you better choose your major?

- Yes
- No

17. Has your favorite class at Dartmouth been in your field of study?

- Yes
- No

18. Has your least favorite class at Dartmouth been in your field of study?

- Yes
- No

19. Do you believe that having distributive requirements contributes to your understanding of your major or that it detracts from it?

- [ ] Augments my major
- [ ] Detracts from my major

20. Do you believe that four years is long enough to prepare you for your field of study?

- Yes
- No

**Figure A6 (continued):** This form was given to the control subjects as their first task during the experiment.
21. On a scale of 1 to 10, how happy do you feel most people are with their choice of major?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not Very Happy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Extremely Happy</td>
</tr>
</tbody>
</table>

22. Do you think it is more important to be skilled in your field of study or genuinely interested in it?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Skilled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Genuinely Interested</td>
</tr>
</tbody>
</table>

23. Do you believe that it is possible to make a wrong choice when choosing your major?

Yes    No

24. In your opinion, what percentage of students at Dartmouth chooses a major that makes them happy?

- 0% - 19%
- 20% - 39%
- 40% - 59%
- 60% - 79%
- 80% - 100%

25. Do you think happiness is an important consideration in how one should select their major?

Yes    No

**Figure A6 (continued):** This form was given to the control subjects as their first task during the experiment.
Facebook Questionnaire

The following questions are related to your Facebook account. Please answer all questions honestly, and to the best of your knowledge.

1. Have you ever looked at your “Privacy Settings” on Facebook?
   Yes  No

2. Have you ever changed any of the settings in your “Privacy Settings”?
   Yes  No

3. On a scale of 1 to 10, how open do you consider your Facebook privacy settings?
   1  2  3  4  5  6  7  8  9  10
   Very Closed   Extremely Open

For the following questions, assume that Facebook has an interface that allows you to easily configure your security settings in any way you want.

4. How would you set the “Search Visibility” for your Facebook account?
   ___ My Networks
   ___ My Networks and Friends of Friends
   ___ My Networks and Friends
   ___ Friends of Friends
   ___ Only Friends
   ___ Custom: ________________________________

5. Who would you allow to view your Profile?
   ___ Everyone
   ___ My Networks and Friends
   ___ People at Dartmouth and Friends
   ___ Friends of Friends
   ___ Only Friends
   ___ Custom: ________________________________

Figure A7: This form was given to the introspective subjects as their first task during the experiment.
6. Who would you allow to view your Basic Info?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

7. Who would you allow to view your Personal Info?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

8. Who would you allow to view your photo albums?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

9. Who would you allow to view your Friends list?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

Figure A7 (continued): This form was given to the introspective subjects as their first task during the experiment.
10. Who would you allow to view the Wall Posts on your profile page?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

11. Who would you allow to view your Education Info?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

12. Who would you allow to view your Work Info?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

13. Who would you allow to view your IM Screen Name?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

Figure A7 (continued): This form was given to the introspective subjects as their first task during the experiment.
14. Who would you allow to view your Mobile Phone Number?

- Everyone
- My Networks and Friends
- People at Dartmouth and Friends
- Friends of Friends
- Only Friends
- Custom: __________________________

15. Who would you allow to view your Current Address?

- Everyone
- My Networks and Friends
- People at Dartmouth and Friends
- Friends of Friends
- Only Friends
- Custom: __________________________

16. Who would you allow to view your Websites?

- Everyone
- My Networks and Friends
- People at Dartmouth and Friends
- Friends of Friends
- Only Friends
- Custom: __________________________

17. Who would you allow to view your Current Residence?

- Everyone
- My Networks and Friends
- People at Dartmouth and Friends
- Friends of Friends
- Only Friends
- Custom: __________________________

**Figure A7 (continued):** This form was given to the introspective subjects as their first task during the experiment.
18. Who would you allow to view your Primary Email Address?

___ Everyone
___ My Networks and Friends
___ People at Dartmouth and Friends
___ Friends of Friends
___ Only Friends
___ Custom: ________________________________

19. Do you limit any of your Facebook friends to only being able to view your Limited Profile?

Yes  No

20. Is there anything on your Facebook account that you would not want an employer to see?

Yes  No

21. Is there anything on your Facebook account that you would not want a parent to see?

Yes  No

22. Is there anything on your Facebook account that you would not want a professor to see?

Yes  No

23. Are you Facebook friends with any professors?

Yes  No

24. Are you Facebook friends with any of your past or present bosses or employers?

Yes  No

25. Does one of your parents have a Facebook account?

Yes  No

**Figure A7 (continued):** This form was given to the introspective subjects as their first task during the experiment.
26. Are you Facebook friends with one of your parents?
   Yes  No

27. Are you Facebook friends with someone you have never met before in real life?
   Yes  No

**Figure A7 (continued):** This form was given to the introspective subjects as their first task during the experiment.
Figure P1: InnerCircle Profile 1 from user study.
Figure P2: InnerCircle Profile 2 from user study.
Figure P3: InnerCircle Profile 3 from user study.
Figure P4: InnerCircle Profile 4 from user study.
Figure P5: InnerCircle Profile 5 from user study.
Figure P6: InnerCircle Profile 6 from user study.
Figure P7: InnerCircle Profile 7 from user study.
Figure P8: InnerCircle Profile 8 from user study.
Figure P9: InnerCircle Profile 9 from user study.
Figure P10: InnerCircle Profile 10 from user study.
Figure P11: InnerCircle Profile 11 from user study.
Figure P12: InnerCircle Profile 12 from user study.
Figure P13: InnerCircle Profile 13 from user study.
Figure P14: InnerCircle Profile 14 from user study.
Figure P15: InnerCircle Profile 15 from user study.
Figure P16: InnerCircle Profile 16 from user study.
**Figure P17**: InnerCircle Profile 17 from user study.
Figure P18: InnerCircle Profile 18 from user study.
**Figure P19:** InnerCircle Profile 19 from user study.
Figure P20: InnerCircle Profile 20 from user study.
Works Cited


Kristol, David M. "HTTP Cookies: Standards, privacy, and politics." ACM Transactions
Masone, Christopher P. "Attribute-Based, Usefully Secure Email." Diss. Dartmouth College, Department of Computer Science, 2008.

Matt Blaze, Joan Figenbaum, John Ioannidis, and Angelos D. Keromytis. The KeyNote trust-management system version 2. RFC 2704, September 1999.


