7-2009

Privacy Risk Assessment Case Studies in Support of SQUARE

Varokas Panusuwan

Prashanth Batlagundu

Software Engineering Institute

Privacy Risk Assessment Case Studies in Support of SQUARE

Varokas Panusuwan
Prashanth Batlagundu

Nancy Mead, Faculty Advisor

July 2009

SPECIAL REPORT
CMU/SEI-2009-SR-017

CERT Program

http://www.sei.cmu.edu

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense and is supported by the Army Research Office through grant number DAAD19-02-1-0389 (“Perpetually Available and Secure Information Systems”) to Carnegie Mellon University’s CyLab. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Table of Contents

List of Figures

List of Tables

Acknowledgments

We appreciate the participation of Gowtham Sridharan, who worked with us on this project and participated in the case study interview process. We also appreciate the assistance of the SEI editorial staff.

Abstract

This report contributes to further development of the Security Quality Requirements Engineering (SQUARE) method to address privacy. Risk assessment is Step 4 in the standard SQUARE process. This report examines privacy definitions, privacy regulations, and risk assessment techniques for privacy. The risk assessment techniques are classified using a standard method, and promising techniques are applied to two case studies. The case study results are provided along with future plans for SQUARE for Privacy.

1 Overview

In this report, we continue to describe extensions to the SQUARE method [Mead 2005] to support privacy. This work builds on earlier extensions to SQUARE in consideration of privacy [Miyasaki 2008a] and is part of a multiyear plan to extend SQUARE in support of privacy (P-SQUARE). Since performing risk assessment is Step 4 of the SQUARE process, it seems natural to examine risk assessment for the special needs of privacy.

Software-intensive systems are widely used for the rapid storage and retrieval of data. We trust that all types of data will reside in these systems and easily be transferred to other systems. This high level of trust poses certain privacy risks for sensitive information. If these risks are identified, we will be able to understand the potential consequences and establish the necessary preventative measures. This report summarizes the assessment of risks while focusing primarily on privacy concerns.

2 Definition of Privacy

It is necessary to clearly define the terms involved in information privacy. Without a clear definition of privacy, it is challenging to draw clear boundaries between general and specialized privacy risk assessments.

We first look at the public dictionary definitions of privacy. These definitions give us a general idea of the term and shed some light on potential meaning conflicts. Next, we look more closely at literature involving privacy risks to understand more about the term, both explicitly and implicitly stated.

2.1 General Definition of Privacy

According to Wikipedia, information privacy is defined as "the relationship between collection and dissemination of data, technology, the public expectation of privacy, and legal issues surrounding them" [Wikipedia n.d.]**.** This source also notes that "privacy concerns exist wherever personally identifiable information is collected and stored—in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues." Detailed information about privacy, including special topics such as internet privacy, can be found on the Wikipedia website.

The definition of privacy differs slightly between two dictionaries. *Merriam-Webster* defines privacy as either "the quality or state of being apart from company or observation" or "freedom from unauthorized intrusion" **[**Merriam-Webster n.d.]**.** The *Oxford English Dictionary* defines privacy as a "state in which one is not observed or disturbed by others" [AskOxford n.d.]**.**

2.2 Privacy as Discussed by Publications and Researchers

2.2.1 Privacy as an Ability to Control Personal Information

In his master's degree thesis, Seiya Miyazaki contrasts two meanings of privacy [Miyazaki 2008b]**.** Privacy is defined by Turkington as "the ability of an individual to control his/her own information" **[**Turkington 1990]. This is very different from the definition "the right to be left alone" as described in [Samuel 1890]**.**

Microsoft published a set of privacy guidelines for software development. In this document, they state that the core principle of the guideline is that "Customers will be empowered to control the collection, use, and distribution of their personal information" [Microsoft 2008].

Altman and Chemers [Altman 1984] conceptualize privacy as a selective control of access to the self. They propose a view of privacy as a process where degree of confidentiality differs depending on the time. They also state that people usually optimize their accessibility along a spectrum of "openness" and "closeness" depending on the operating context.

2.2.2 Privacy as Freedom from Unauthorized Intrusion

In a study to experiment with a lightweight method helping in privacy-oriented requirements elicitation, Jensen and Potts refer to "privacy enhancing principle (i.e., information minimization)" that could augment the requirements **[**Jensen 2007]. The suggested technique to enhance privacy in this case implies that we could establish measures to guarantee the security of data. This paper views privacy as freedom from unauthorized intrusion.

In a study to create a model to monetize the value of privacy data, Yassine and Shirmonhammadi state that there should be a way to help "regulate the use and the disclosure of confidential information so that consumers' right to privacy is protected" [Yassine 2008]. The model also seems to be based on preventing the user's data from falling into the hands of a malicious third party.

Several laws and regulations are written in terms of protecting the privacy of the consumers or service users. However, they do not usually explicitly state the meaning of privacy but rather define entities to be protected and measures required to be implemented. For instance, the Federal Privacy Act's purpose could be summarized as "primarily directed to Federal agencies for the purpose of protecting the privacy of individuals identified in information systems maintained by such Federal Agencies" [University of California 1992].

Unlike many other information privacy related laws, the *Privacy Impact Assessment Guide* published by Australia's Office of the Privacy Commissioner has a defined meaning of privacy. The guide states that information privacy is "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" [OPC 2006].

2.2.3 Relationship Between Privacy and Security

With the definitions above, one can see that privacy involves security concerns, especially if we take the meaning that involves protecting information from unauthorized sources. In one paper discussing privacy risk assessment of a ubiquitous computing system, Hong et al. explain the relationship between security and privacy. They cite the work of Saltzer and Schroeder, which defines security as "mechanisms and techniques that control who may use or modify the computer or the information stored in it" and privacy as "the ability of an individual (or organization) to decide whether, when, and to whom personal (or organizational) information is released" [Hong 2004].

Given this definition, it is clear that security may be one of the key components to ensure that a user can restrict access from certain sources. However, we can see that it is not sufficient to grant total control to the user.

3 Definition of Privacy for Risk Assessment

As we can see from various works, there is no universally agreed upon definition of privacy. Even the works that address information privacy specifically still have some conflicts about its meaning. Papers about risk assessment tend to focus more on controlling personal information than on limiting access.

While there is no significant drawback to the traditional meaning of privacy, it is limiting for the purpose of risk assessment. As stated in their paper about privacy methods, IaChello and Abowd commented that "these efforts have usually taken a normative and systems-oriented, rather than a user-centered, approach and have served well to regulate industrial uses of personal data" [IaChello 2008].

In this report, we take the dynamic meaning of privacy as a freedom to control an individual's information. We do not attempt to regulate how the personal information is used but rather to understand the privacy implications of data being stored and transferred in the system. This meaning is compatible with most literature on the subject.

4 Risk Assessment Methods

We conducted a search of two types of sources for risk assessment methods. We reviewed academic papers that were written specifically to address privacy risk assessment or related issues, and we browsed privacy regulations looking for sections that implicitly or explicitly address the assessment of privacy issues.

4.1 Literature Review

In "Privacy and the Market for Private Data," Yassine and Shirmohammadi discuss approaches to capitalizing private data assets [Yassine 2008]. They propose a model of privacy data negotiation between buyers and sellers. This means that protection of privacy data is necessary only if there is a group driven to buy the information.

In the context of medical patient information, Buffet and Kosa present an analysis of risk in two dimensions: probability and utility [Buffett 2006].

- *Probability* is the likelihood of a patient to indicate certain information. It can come from inference from the proportion of total number of patients who think that privacy is important.
- *Utility* is the personal importance that the patient gives to each information item.

While primarily addressing security issues, the Microsoft Security Development Lifecycle (SDL) also includes privacy risk assessment as part of the development process [Microsoft 2009b]. In the early phases of the lifecycle, the system is divided into different privacy levels. In the later phase, an analysis is conducted based upon privacy level.

- In stage 2, cost analysis, a base questionnaire is given to rate the privacy impact of the system. The system is given a privacy impact rating (P1, P2, or P3), which "measures the sensitivity of the data your software will process from a privacy point of view."
- In stage 4, risk analysis, a detailed privacy analysis is conducted of a project's key privacy aspects [Microsoft 2009a].

With an approach similar to that presented by Microsoft, the *Privacy Impact Assessment Guide* defines a threshold assessment to evaluate the system's overall privacy concerns [OPC 2006]. The purpose of the assessment is to determine whether the level of privacy requirements in the system necessitate a full privacy impact assessment. The report states, "The first critical question in assessing whether a PIA is needed is whether any personal information will be collected, used or disclosed in the project. If personal information is not involved in the project at any stage, the project may have a negligible impact on information privacy and a PIA may not be necessary."

The principle of proportionality is discussed by IaChello and Abowd as a balance between privacy concerns and the utility of the application [IaChello 2005]. They also develop this idea into a method that is used to aid HCI designers in designing applications with complex privacy implications. It has four steps, which complete a cycle.

1. Determine the application goals. (The stakeholders also need to agree on the burden of privacy issues and the benefits of addressing those issues.)
2. Select the appropriate techniques or technologies to use.

3. Validate whether the technologies chosen are adequate for the purpose.
4. Refine the goals and start a new cycle if necessary.

Palen and Dourish suggest a concept of "genres of disclosure," which is another framework to aid the design of a system with privacy concerns. It is based on the observation that "privacy is not simply a problem of access control, but is rather an ongoing and organic process of negotiating boundaries of disclosure, identity, and time" [Palen 2003]. They presented multiple case studies to support the idea that dynamic policies based on circumstances are more effective than static policies that always hold true.

Jensen compares and contrasts different methods in addressing privacy risk concerns when designing software-intensive systems [Jensen 2007].This includes his PhD dissertation, the STRAP method [Jensen 2005].

Hong et al. propose a model for designing ubiquitous computing systems with privacy concerns [Hong 2004]. They address both privacy risk analysis and management. The goal of this model is "to help elucidate those needs and trust levels, refining privacy from abstract principles into concrete issues that can be acted upon in specific domains for specific apps." The analysis is done by using series of questions to elicit requirements. The same authors also wrote a paper on pitfalls for designers of systems with privacy concerns [Lederer 2003].

The Treasury Board of Canada's Privacy Impact Assessment Guidelines can be used as a framework in eliciting privacy requirements. The framework is composed of three parts: need assessment, documenting the data flow, and privacy analysis [TBCS 2002].

A model of privacy breaches caused by human error is presented in [Divakaran 2009]. The authors apply the human error model to the system privacy model and identify possible issues.

The CERT OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation℠) method is a collection of frameworks and security assessment methods using a risk-based approach. In the background section of a practitioners report [Woody 2006], it is noted that OCTAVE was developed to "apply the approach to the security compliance challenges faced by the U.S. Department of Defense (DoD) when the security compliance portion of the Health Insurance Portability and Accountability Act (HIPAA) was mandated." Since HIPAA deals directly with information privacy, the tools and methods presented in OCTAVE could be useful in our case as well. Specific practices can also be found in the *OCTAVE Catalogue of Practices* [Alberts 2001].

4.2 Privacy Regulations

Besides academic literature on privacy risk assessments, many laws and regulations provide a set of guidelines that can be used to assess privacy risks. However, some literature argues that the guidelines usually address the system as a whole but not the interaction between different parties passing sensitive information. Some guidelines also seem to follow a different meaning of priva-

® OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University. Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

cy, as stated in the previous section. This is evident in certain cases where the objective is stated clearly to "protect privacy" rather than to empower the user's control of the information.

Although not ideal, the guidelines provided by different institutions give diverse viewpoints on the problem of privacy risk assessment. Looking at these guidelines, we also gain insight into the components of privacy risk assessments which can be used to find opportunities for improvements.

4.2.1 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) addresses privacy concerns of health information systems by enforcing data exchange standards. The act also provides a guideline to analyze risks. The overall objective of a HIPAA risk analysis is to document the potential risks and vulnerabilities related to the confidentiality, integrity, and availability of electronic protected health information (ePHI) and to determine the appropriate safeguards to bring the level of risk to an acceptable and manageable level. Risks found by the analysis fall into three categories: access, storage, and transmission.

The entities of interest in HIPAA are called the "Covered Entities" (CEs), which must comply with the HIPAA Security Rule. These are health plans (HMOs, group health plans, etc.), health care clearinghouses (billing and repricing companies, etc.), and health care providers (doctors, dentists, hospitals, etc.) that transmit any ePHI.

There are seven steps in HIPAA risk assessment:

1. Inventory and classify assets.
2. Document likely threats to each asset.
3. Conduct a vulnerability assessment.
4. Evaluate current safeguards (administrative, physical, and technical).
5. Document risks.
6. Recommend appropriate safeguards.
7. Report on results.

4.2.2 Public Records Act

The Public Records Act (PRA) states that every person has a right to inspect any public record, with specified exceptions. A University Electronic Communications Record, for example, is a public record whether or not any of the electronic communications resources used to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print the record are owned by the university. The university's online service providers must have procedures for making their records available in accordance with any requests under the PRA, other laws, or as a result of litigation.

This act demonstrates another view of privacy, as the aim is not solely an attempt to protect privacy but to define it in terms of access granted to certain parties involved in the information of interest.

References

http://comp-resources.berkeley.edu/privacy/regulations.html
http://www.atg.wa.gov/OpenGovernment/InternetManual/Chapter2.aspx

4.2.3 The Family Educational Rights and Privacy Act

Family Educational Rights and Privacy Act (FERPA) regulations provide that educational agencies and institutions that receive funding under a program administered by the U. S. Department of Education must provide students with access to their education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records. With several exceptions, schools must have students' consent prior to the disclosure of education records. Examples of situations affected by FERPA include school employees divulging information to someone other than a child's parents about the child's grades or behavior, and school work posted on a bulletin board with a grade.

References
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
http://en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act

4.2.4 Electronic Communications Policy

A set of rules is published by University of California addressing a privacy concern in electronic communication. The purposes of this policy are to establish guidelines on privacy, confidentiality, and security in electronic communications. Items to be protected in this case are personal information, student information, electronically gathered data, and telephone conversations. The regulations identify the entities that are allowed access to information and those that must be restricted from it.

References
http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#PROVISIONS

4.2.5 Gramm-Leach-Bliley Act

The main purpose of this act is to allow commercial and investment banks to consolidate as one institution. As the banks are merged, the act also specifies certain regulations regarding financial information privacy. These are the three main components of this act that address privacy:

- **Financial Privacy Rule.** A financial institution must give its customers privacy notices that explain the institution's information collection and sharing practices. This privacy notice must be given to customers before any business agreements can be made.
- **Safeguards Rule.** The institution must create a security plan to protect the confidentiality and integrity of personal consumer information.
- **Pretexting Protection.** The institution must protect personal information from access without an authority. This could also be referred to as protection from social engineering.

For a privacy dimension of this act, financial institutions must provide their clients a privacy notice that explains what information the company gathers about the client. The responsibility is not just explaining the changes but also giving the customer the opportunity to opt out. This means that customer can say "no" to allowing their information to be shared. However, there are also items that customers cannot choose to opt out of:

- information shared with those providing priority service to the financial institution
- marketing of products and services for the financial institution
- information that is deemed legally required

This law also made a reference to the Fair Credit Reporting Act, stating that the privacy notice needs to identify the right to opt out to unaffiliated parties.

References
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
FAQ on GLBA http://www.ftc.gov/privacy/glbact/glb-faq.htm

4.2.6 Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) directly regulates the collection, dissemination, and use of consumer credit. Combined with the Fair Debt Collection Practices Act, the FCRA defines rights to credit information. It mainly regulates how consumer reporting agencies operate. A few statements addressing privacy concerns are

> "If negative information is removed as a result of a consumer's dispute, it may not be reinserted…"
>
> "Credit Reporting Agencies may not retain negative information for an excessive period."

As stated in the above section, this law complements the Gramm-Leach-Bliley Act by addressing sharing information with third parties.

4.2.7 Campus Mailing List Regulations

Electronic mail certainly is another form of digital data transfer. Special care must be given to email that has the potential to be viewed by many parties. Different universities state their regulations differently. For example, University of California at Berkeley regulations state that

> "Mailing list managers must provide the means for subscribers to find out what level of privacy protection is normally available for addressee names included on the list."
>
> "List managers also must advise their list members that despite whatever settings are in place for normal access could result in disclosure of list membership information."

Reference
http://comp-resources.berkeley.edu/privacy/privacy-guidelines.html

4.2.8 The Patient Safety and Quality Improvement Act of 2005

This law creates "Patient Safety Organizations (PSOs) to collect, aggregate, and analyze confidential information reported by health care providers." The act is a direct response to the fear of letting federal agencies have access to patient records.

The interesting characteristic of this law as opposed to others is that it does not attempt to regulate any private entities. Rather, it defines how the U.S. government will operate on sensitive patient information so as to provide transparency in the process.

References
http://www.ahrq.gov/qual/psoact.htm
http://www.pso.ahrq.gov/statute/pl109-41.htm

4.2.9 Fair Information Practices Act

The intent of the Fair Information Practices Act (FIPA), a Massachusetts state law, is to ensure that certain types of personal data collected and held by the state government remain private and are disclosed only in accordance with applicable law. FIPA also extends to certain individuals' rights over pertinent state-held data.

The general idea of this act exhibits a strong correlation to the Patient Safety Act. Both laws are not used to regulate any other entity but the government itself. FIPA was passed to ensure that the government would not abuse the privacy of its citizens. It also grants an authorization to certain agencies to issue further regulations.

References

http://www.umass.edu/humres/library/fipa.htm
http://www.mass.gov/Ihqcc/docs/meetings/08feb20_presentation_fipa_hipaa.ppt

5 Elements of Privacy Risk Assessment

As one can observe, several aspects of privacy risk assessment addressed in the academic literature and the laws above tend to focus on a certain area of interest. To be able to formulate a framework for privacy risk assessment, we need a complete view of the process.

We need a way to classify each piece of literature into an area of concern in risk assessment. According to Barry Boehm, risk assessment has three major components [Boehm 1991]:

1. Risk Identification. The project-specific risks are generated using various identification techniques.
2. Risk Analysis. After risks are detected in the identification step, certain properties are assigned to each risk statement so that they can be distinguished by group.
3. Risk Prioritization. A ranked order of risks is produced in order to show their importance.

Using these steps as a guideline, we classify each document by the components of risk assessment it addresses. (See Table 1 and the classification scheme that follows it.) We can then select the pieces and assemble a complete risk assessment technique.

Table 1: Classification of Papers and Regulations by Risk Assessment Category

Type	Publication / Regulation (numbers correspond to classification details below)
Risk Identification	[3][4][5][6][7][8][9][10][11][12][16][17]
Risk Analysis	[1][2][4][7][8][9][11][13][14][15][18],[19],[20]
Risk Prioritization	[1][7][8]

5.1 Classification Details

1. Privacy and the Market for Private Data: A Negotiation Model to Capitalize on Private Data
   - See Section 5.2 - Data Classifications and Risk Quantification.
   - In Section 6, the authors use game theory to model the relationship between information buyers and sellers.
2. Towards a Model for Risk and Consent Management of Private Health Information
   - See Section V - Risk Analysis.
3. Microsoft Security Development Lifecycle (SDL)
   - For Stage 2: Cost Analysis - Privacy Requirements, we need to classify the system into one of the three privacy levels.
   - For Stage 4: Conduct Risk Analysis based on privacy level.
4. Privacy Impact Assessment Guide
   - Section 14 demonstrates how to map the information flow in the system.
   - Section 15 presents a series of questions used to elicit areas of risk but provides no guidance on how to prioritize them.
5. Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design In Ubiquitous Computing
   - Explains the principle of proportionality in relation to privacy.
6. Unpacking “Privacy” for a Networked World

- Provides a general understanding that privacy requirements are dynamic.

7. Experimental Evaluation of a Lightweight Method for Augmenting Requirements Analysis
   - Proposes the STRAP method for assessing privacy risks and guiding the design process.
8. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems
   - Proposes a complete privacy risk model for ubiquitous computing.
9. Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks
   - Presents a data flow table.
   - Discusses privacy analysis in a separate section.
10. How Significant Is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management
    - This is not directly related to risk; it considers human errors that cause privacy breaches. However, we might have a way to map human error behavior onto risk.
11. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
12. Health Insurance Portability and Accountability Act (HIPAA)
13. Public Records Act (PRA)
14. The Family Educational Rights and Privacy Act (FERPA)
15. Electronic Communications Policy
16. Gramm-Leach-Bliley Act
17. Fair Credit Reporting Act (FCRA)
18. Campus Mailing List Regulations
19. The Patient Safety and Quality Improvement Act of 2005
20. Fair Information Practices Act (FIPA)

6 Case Studies

6.1 Case Study 1

A research-oriented school in a university needs a tool to help manage the awards that they receive for research activities. A research activity is one that will advance the knowledge in the discipline; an award is a grant that is given to the researcher to conduct the research. The tool is expected to help researchers and their business manager in

- handling the proposal process for winning awards
- importing human resources and accounting data to aid in forecasting
- tracking and forecasting the amount of funding spent
- certifying the effort of the researchers that work on a research activity

In order to create a proposal and do the forecasting, the system needs to use this data:

- HR data, including salaries and effort of each staff member
- nature of the research in the proposal

6.2 Case Study 2

A fitness consulting firm that provides health fitness solutions to its clients collects the testing data of the clients and recommends a coaching program based on their metabolic activity. The project basically involves the development of a web-based application to automate the following processes:

- collecting medical data
- managing the database
- providing customized reports of patient data

The following are the types of data handled through the application:

- heart rate, blood pressure, metabolic activity
- body measurements such as height, weight, and girth
- food patterns (breakfast time, lunch time and dinner time)

7 Selected Risk Assessment Techniques

One of the techniques used for both of the above-mentioned projects was the risk model developed for ubiquitous computing. The model is composed of two parts. The first is a risk analysis that poses a series of questions to help designers refine their understanding of the problem space. The second part looks at privacy risk management, which deals with categorizing, prioritizing, and developing interaction techniques, architectures, and strategies for managing potential privacy risks.

7.1 Privacy Risk Analysis for Ubiquitous Computing

The first part of the privacy risk model is a set of questions intended to help design teams think through specific privacy issues for ubiquitous computing applications. The output from this analysis should be an unordered list of potential privacy risks. The questions are organized into two groups, looking at the social and organizational context in which the application is embedded and the technology used in implementing that application.

The second part of the privacy risk model looks at privacy risk management, which takes the unordered list of privacy risks from the privacy risk analysis, prioritizes them, and helps design teams identify solutions for helping end users manage those issues (through technical solutions, social processes, or other means). This privacy risk management is based on the concept of reasonable care in law: "the degree of care that makes sense and that is prudent, enough but not too much" [Feinman 2000]. This model uses Hand's cost-benefit analysis [Hand 1947], which considers three factors for use in managing privacy:

1. the likelihood L that an unwanted disclosure of personal information occurs
2. the damage D that will happen on such a disclosure
3. the cost C of adequate privacy protection

This model also proposes to use a qualitative assessment of high, medium, and low to help gauge each of these factors, though we used a numerical scale to quantify the values. In general, situations where C < LD, that is, where the risk and damage of an unwanted disclosure outweigh the costs of protection, suggest that privacy protections should be implemented.

After identifying and prioritizing the privacy risks (based on likelihood and damage), it is useful to think about how to manage those risks.

7.1.1 Case Study 1 - Proposal Tool

In the interview, a series of questions were posed to the project representative. A summary of the interview is given below.

Data observer: Sponsor's project accountant

Direct users: Business manager (BM), project implementer (PI), administrator

Data sharers: PI and BM share data with each other; dean and Office of Sponsored Projects (OSP) shares data with accountant

Information shared: Address, salary, and effort of each employee

When it is shared: When the budget is sent for approval

Relationship between data observers, sharers: PI and BM, social; sponsor and OSP, legal

Malicious observers: Credit card, marketing, and financial companies might be interested in salary data; competitors might be interested in project data

Stakeholders: Researchers, part-time programmers, staff who will conduct each proposed project

Data retention: Permanent

As part of the risk analysis, the first step is to identify the risks. The following were the risks identified after the interview.

1. Data is being shared with the OSP users and it is not clear who the users are. The information might end up being shared with untrusted users.
2. Sharers' addresses, salaries, and effort on each project are being uploaded to a website, which might cause the information to be pulled by malicious users.
3. There are no incentives for protecting personal information.
4. The university's competitors could be the malicious observers that may end up giving out information to credit card companies and marketing companies, which in turn will result in loss of business to the university.
5. Data that is permanently stored on university servers might result in information being pulled from present and past projects.

After identifying and agreeing with the identified risks, the team, along with the project representative, discussed the risks and then prioritized them using Hand's cost-benefit analysis.

The following values were used for prioritizing the risks.

Likelihood and damage

3 - High

2 - Med

1 - Low

Cost

Cost values range from 1–9, where 1 means the cost of implementing measures is low and 9 means it is very high.

Risk ID	Likelihood	Damage	Cost
1	2	3	4
2	2	3	7
3	3	3	6
4	1	3	4
5	1	3	8

Likelihood and damage values were determined by the project representative, and the cost values were determined by the team.

7.1.2 Case Study 2 – Fitness Consulting Tool

In the interview, a series of questions were posed to the project representative. A summary of the interview is given below.

Data observer: Case manager, dietician, exercise specialist, and administrator (has access to the database)

Direct users: Case manager (testing and data), dietician (analysis and recommendations), exercise specialist (suggesting exercise routines)

Data sharer: Patient

Information shared: Measurements, date of birth, first name and last name, and other testing details such as heart rate

Circumstance under which data is shared: When the patient wants recommendations, the case manger enters the data; once the data is in the database, others users can view the data

Malicious observers: None

Data is shared because: More testing values lead to more recommendations

Incentives for protecting data: They might lose business if customers sue or lose trust

Level of trust of people who are sharing the information: Business relationship

Kind of personal information people might be interested in: Date of birth, first and last name, testing details

Data retention: 12 months (after that, the client doesn't know what is done with the data)

Personal information collection source: Web-enabled user interface and external device that is fixed to the body. Main entry point: case manager enters data into the system on behalf of the client. One way is manual and other is automated.

Who has control? Three users, and system admin has control of the database

How it is shared? Case manager enters the data and then other users view the data from the entered source

Push or pull? Case manager pushes the data and others users can pull the required information

Opt in or opt out? Data sharers can view only the required data (depending on the visiting patient)

Information sharing? Patient details can be viewed by the case manager at any time

Data uploading? Continuous and done at various times

Data storage? Office location

Access to data location? System admin

The first step in the risk analysis is to identify the risks. The following were the risks identified after the interview.

1. All data observers have access to many types of personal information of the patient and might cause the information to be used inappropriately.
2. All personal information shared is static information, which might result in revealing the user's identity.
3. There is no value proposition for all the data observers to share the patient's personal information; the exercise specialist, dietitian, or administrator may give the information to outside users.
4. Collecting data sharers' information through network-based or network-assisted approaches might result in less security protection of the users' information.
5. A pull mechanism is used, so it introduces more risk and might result in all of a user's information being retrieved from the database.
6. The data retention period is defined, but after that the client does not clearly know what will happen to the data. Information of present and past clients might be pulled.

After identifying and agreeing with the identified risks, the team, along with the project representative, prioritized the risks using Hand's cost-benefit analysis.

The following values were used for prioritizing the risks.

Likelihood and damage

3 - High

2 - Med

1 - Low

Cost

Cost values range from 1–9, where 1 means the cost of implementing measures is low and 9 means it is very high.

Risk ID	Likelihood	Damage	Cost
1	2	3	4
2	2	2	6
3	3	2	8
4	3	3	3
5	3	3	4
6	3	3	3

Likelihood and damage values were determined by the project representative, and the cost values were determined by the team.

7.1.3 Reflections

This approach only expresses what factors should be taken into account. The values of these factors are judgment calls based on the best knowledge that the design team has.

This approach does not address extreme cases; instead it looks at risks that are foreseeable and significant.

The utility of this cost-benefit analysis comes not so much from accurate and precise values as from having the design team think through the issues of likelihood, damage, and cost.

This approach addresses relatively few security issues. It should be used in conjunction with a security threat model to ensure that the desired privacy needs are properly implemented and secured.

7.2 Structured Analysis of Privacy

The second risk assessment methodology we adopted was the Structured Analysis of Privacy (STRAP) methodology. STRAP is designed to strike a balance between the robustness of requirements engineering based techniques and the flexibility and ease of use of heuristics-based approaches. STRAP combines these two methods, goal-oriented analysis and heuristic evaluation, in an effort to improve the quality and effectiveness of the analysis while keeping the costs down.

STRAP is primarily aimed at supporting designers and analysts in dealing with privacy in the early phases of design when functionality is still being decided and fundamental design decisions can still be changed or influenced. STRAP is also specifically aimed at dealing with the HCI problems associated with privacy awareness and management. This means that the heuristics used are specifically targeted to dealing with these issues. This does not mean that STRAP will not be useful in analyzing and discovering other types of privacy problems, although this is a question that will have to be determined experimentally.

Specifically, STRAP uses a goal-oriented analysis technique to structure the problem space, ensuring a thorough and balanced analysis, and uses lightweight and efficient heuristics to identify potential privacy problems, suggest solutions or design refinements, and finally help the analysts evaluate these refinements.

7.2.1 Goal-Oriented Analysis in STRAP

Goal-oriented analysis is a technique typically associated with requirements engineering [Dardenne 1993]. It is used to elicit system requirements and structure how analysts and designers think about a system early in the design process. In goal-oriented analysis, the analyst identifies the systems goals from a users' perspective by studying users and the way they interact with each other, the systems, artifacts, and the environment. From these observations, requirements can be identified, either directly or by deriving scenarios and use cases which illustrate typical as well as critical functions or tasks. In this role, goal-oriented analysis can be used to structure and analyze complex sets of observational or unstructured data. After identifying key goals and functions, these are broken down into increasingly simple component subgoals, much in the same way as in the GOMS method [John 1996]. This process continues until the subgoals are trivially simple and further breakdown is counterproductive. An alternative definition of how far a set of goals need to be decomposed is that all leaf-goals must be assignable to a single actor. In other words, all leaf-goals must be so simple that a single entity or system can fulfill them completely. Until the analysis reaches this level, implementation details and necessary decisions will likely be hidden or lost in the analysis.

7.2.2 Vulnerability Analysis Using STRAP

Using the goal tree derived in the previous step as a blueprint or checklist of the functionality to consider, an analyst can set out to identify potential privacy vulnerabilities. Both heuristic-based and requirements engineering analysis methods commonly rely on a small set of analytical questions to identify potential problems (see Figure 6 in [Bellotti 1993] or Figure 7 in [Hong 2004] for examples). For STRAP, these questions were derived from Bellotti and Sellen, as well as a review of the information life cycle, potential sources of information misuse, and the kinds of questions users have about companies' information practices.[1] For each goal and subgoal, the designer should ask the following questions to determine the information capture and use:

- What information is captured, accessed, processed, transmitted, received, or stored in meeting this goal?
- How is the information captured, accessed, processed, transmitted, received, or stored?
- Who are the actors involved in the capture, access, processing, transmission, receipt, or storage?
- What knowledge is derived from this information?
- What is done with the information and meta-information after the goal is met?

If information is captured, accessed, processed, transmitted, received, or stored, this may present privacy vulnerability. Vulnerabilities are marked in the goal tree as clouds over the path to the goal. By placing these vulnerabilities in the diagram, we preserve context information; we know what goals these problems are associated with and what actors are involved. This helps give the designers, programmers, and users a shared vocabulary for discussing the system. Furthermore, when goals are finally translated into requirements, functions, and eventually system components, we can trace how these vulnerabilities are addressed or will affect different system components.

[1] Earp, J. B. & Meyer, G. "Internet Consumer Behavior: Privacy and its Impact on Internet Policy," 28th Telecommunications Policy Research Conference, September 2000.

Once vulnerabilities have been identified, we look for common causes and duplicate vulnerabilities. These often occur when one set of goals collect, transmit, or store data needed to meet a different set of goals. The vulnerability will then appear in two or more places on the goal tree, with different contexts. If the vulnerability associated with the transmission of data is addressed through the encryption of that data, then the vulnerability associated with receiving the information will also be addressed. These duplicates are important to identify, not simply because it simplifies the analyst's job later on, reducing the number of vulnerabilities to address, but because it affects the cost-benefit analysis which should be a part of the decision about which issues to address.

7.2.3 Case Study 1 – Proposal Tool

Create Goal Tree

Since there were complex interactions between various users in this system, the development team originally used contextual design [Beyer 1998] as an elicitation technique. We found that the sequence diagram helped in constructing the goal tree. The activity and intent column of the sequence model intuitively maps to each goal and subgoal, as shown in Figure 1.

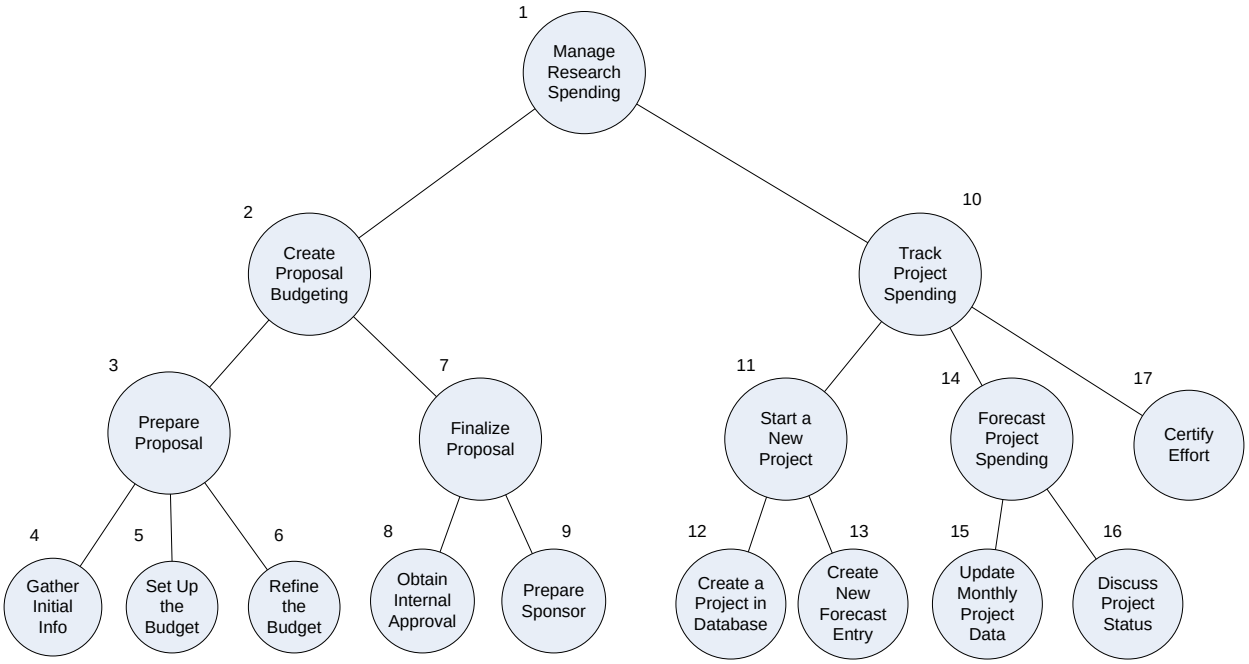

Figure 1: Goal Tree Constructed for Case Study 1

Goal 4: Gather Initial Information

What?	Project name, principal investigators, details of the project known to date
How?	Email
Who?	Principal investigator

Derived Knowledge?	Salary of PI, nature of research for each PI
Activities performed after data collection	Cross check the requirements with sponsor's website

Goal 5: Set Up the Budget

What?	Project spending budget
How?	Look at the published standard rates and posted salary list
Who?	Business manager
Derived Knowledge?	The university's research spending for each department
Activities performed after data collection	-

Goal 6: Refine the Budget

What?	Project spending budget
How?	Email to the PI
Who?	Business manager
Derived Knowledge?	The university's research spending for each department
Activities performed after data collection	-

Goal 8: Obtain Internal Approval

What?	Project spending budget; list of personnel involved
How?	Send a printed package to the office of the project sponsor
Who?	Business manager, office of project sponsor
Derived Knowledge?	The university's research spending for each department
Activities performed after data	Check validity of the proposed project budget

collection	

Goal 9: Prepare Sponsor Information

What?	Project spending budget, list of personnel involved, budget justification
How?	Apply via website
Who?	Business manager, principal investigator
Derived Know-ledge?	Techniques that will be use to approach particular problems; research spending for each project and PI's salary
Activities per-formed after data collection	-

Goal 12: Create a Project in Database

What?	Project schedule and equipment lists
How?	Telephone
Who?	Business manager, office of accounting staff
Derived Know-ledge?	All equipment essential to the success of the research; project schedule
Activities per-formed after data collection	Create an entry in the database for project tracking

Goal 15: Update Monthly Project Data

What?	Monthly project spending data
How?	Published reports or database query
Who?	Business manager, office of accounting staff
Derived Know-ledge?	All equipment essential to the success of the research; project schedule
Activities per-formed after data collection	Create an entry in the database for project tracking

Goal 16: Discuss Project Status

What?	Project spending data to date
How?	Discussion
Who?	Business manager, principal investigator
Derived Know-ledge?	Overall project status; prediction of success or failure of the project
Activities per-formed after data collection	Make adjustments to a project's budget as necessary

Goal 17: Certify Effort

What?	Reported effort data
How?	Report by the database system
Who?	Business manager, principal investigator
Derived Know-ledge?	Predict personnel schedule
Activities per-formed after data collection	-

Apply Design Heuristics

After analyzing vulnerabilities in performing each goal, we can apply design heuristics on them, as shown in Figure 2.

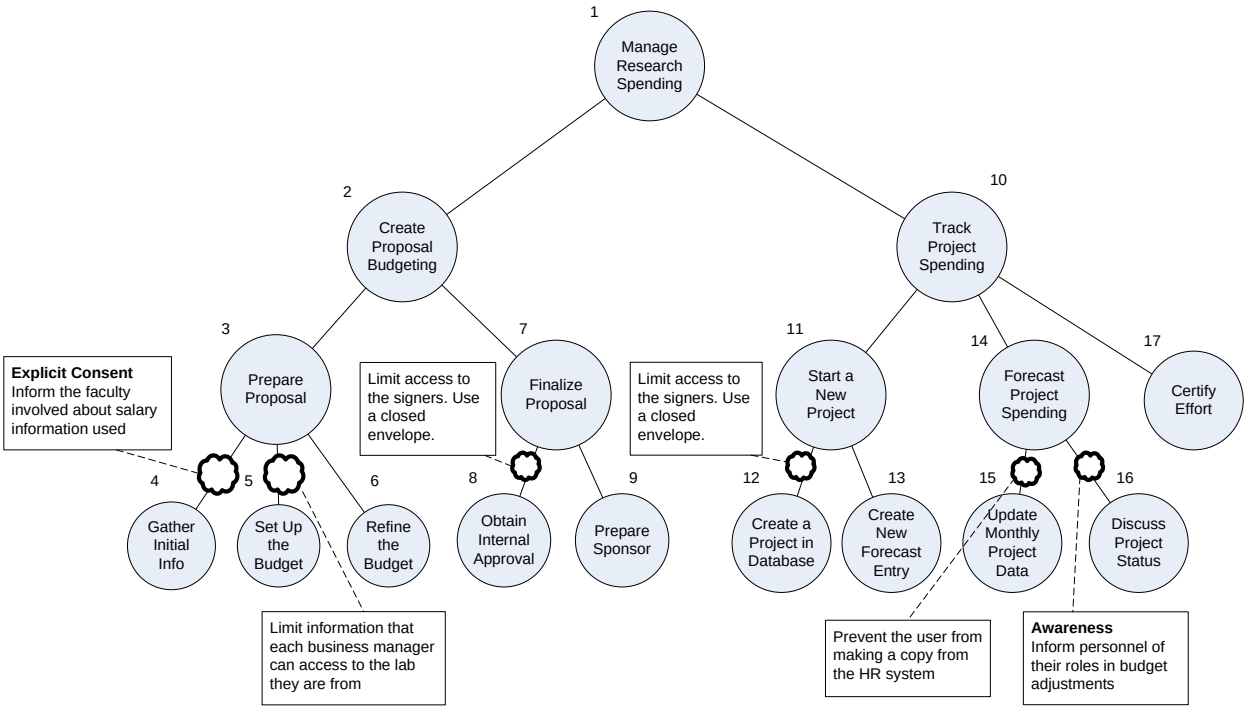

Figure 2: Goal Tree for Case Study 1 with Design Heuristics Applied

7.2.4 Case Study 2 – Fitness Consulting Tool

Create Goal Tree

The goal tree for this case study, as opposed to case study 1, needed to be created from scratch. We conducted an informal interview with the system's developer and documented the goal tree shown in Figure 3.

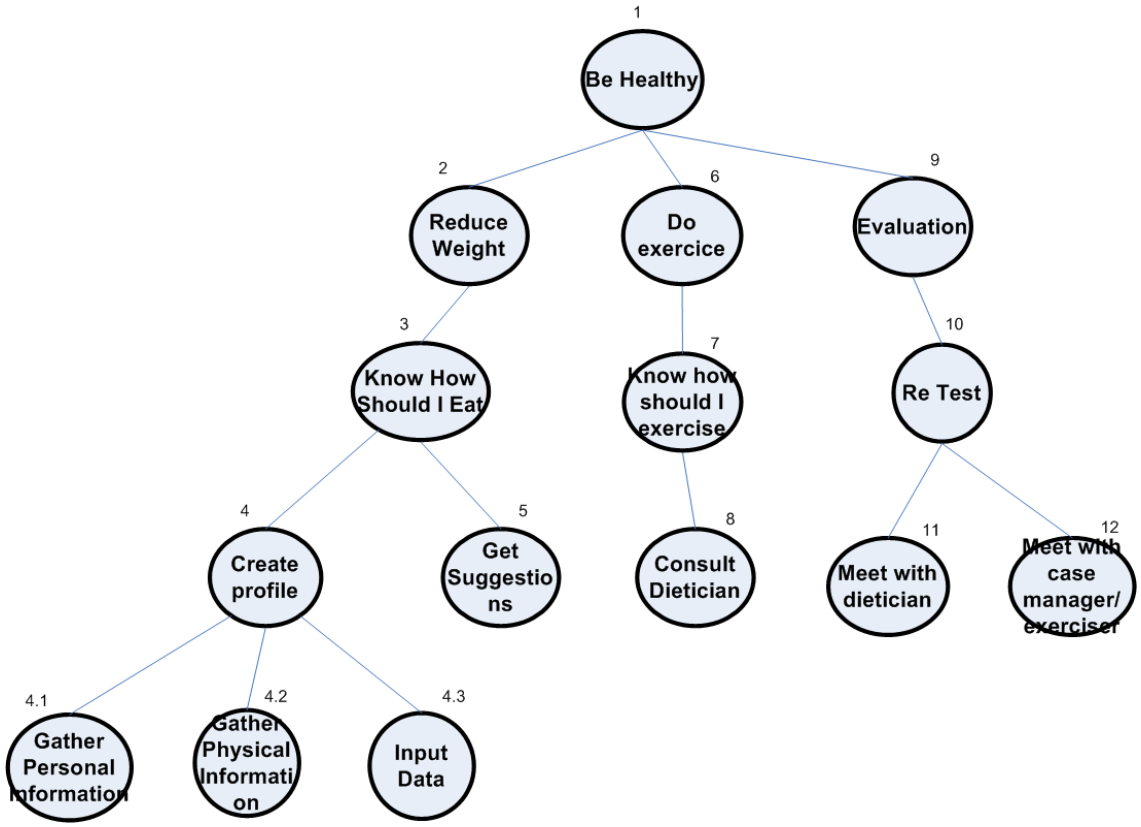

Figure 3: Goal Tree of Case Study 2, Elicited from the System's Developers

Capture Vulnerabilities

Goal 4.1: Gather Personal Information

What?	First name, last name, birth date, gender
How?	Talking to clients
Who?	Case manager, client
Derived knowledge?	(Does not have sufficient domain knowledge to answer questions)
Activities performed after data collection	-
Activities performed after data collection	-

Goal 4.2: Gather Physical Information

What?	Height, weight, breathing measurements, heart rate
How?	Using instruments to measure

Who?	Case manager, client
Derived knowledge?	(Does not have sufficient domain knowledge to answer questions) Personal data for insurance company, perhaps?
Activities performed after data collection	Use this data to analyze the exercise and diets for the patient

Goal 4.3: Input Data

What?	All data from goals 4.1 and 4.2
How?	Manual entry to the system Download from the equipment to Excel file and upload Excel file to the system Report out for the patient
Who?	Case Manager
Derived knowledge?	(Does not have sufficient domain knowledge to answer questions) Personal data for insurance company, perhaps?
Activities performed after data collection	Use the data to analyze the exercise and diets for the patient
Notes	The data could reside in the devices. The only data that is on the device are measured data and gender.

Goal 8: Consult Dietician

What?	All information from goal 4.3; collect food preferences
How?	View the information through the system web interface Can only view, but not edit Manual entry of food preferences into the system
Who?	Dietician and patient
Derived knowledge?	The diet preferences of the patient
Activities performed after data collection	Use other external resources for calculations; provide consulting
Notes	

Apply Design Heuristics

After analyzing the goals, we annotated the goal tree with suggested design heuristics to address each goal's specific problem, as shown in Figure 4.

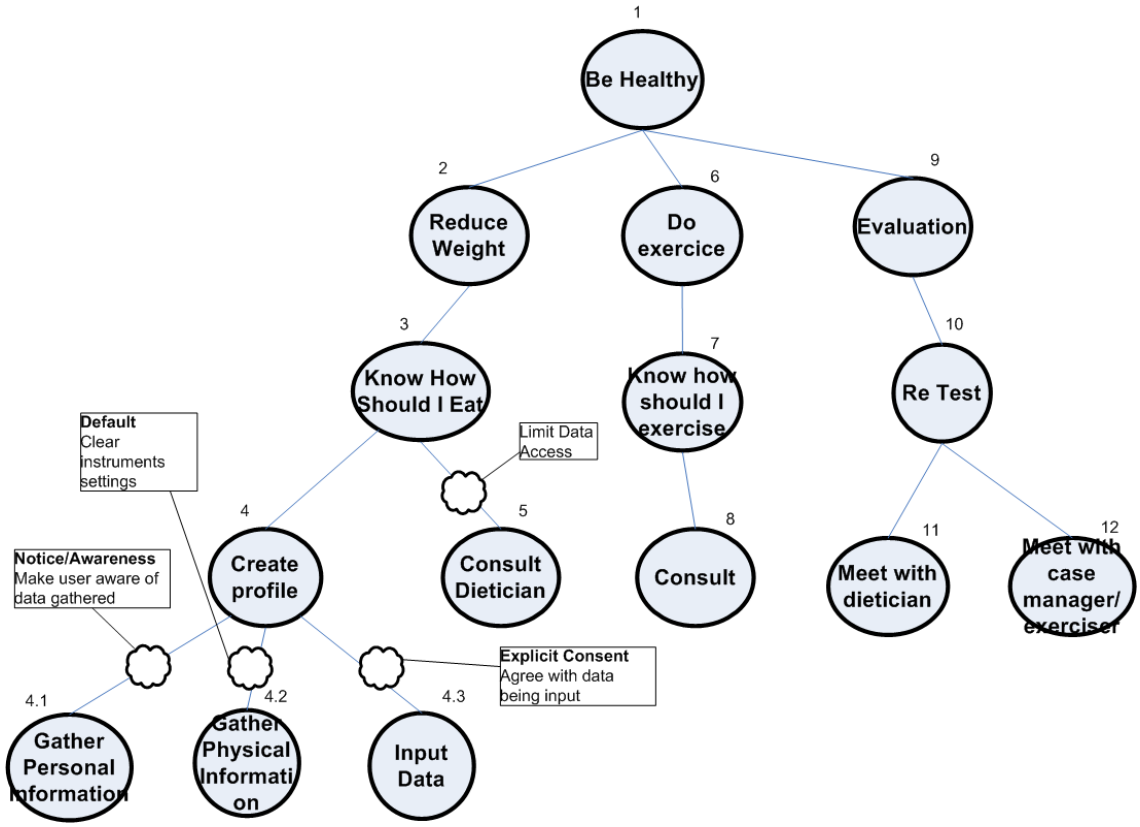

Figure 4: Goal Tree for Case Study 2 with Design Heuristics Applied

7.2.5 Reflections

This approach did not address how to prioritize the identified risks.

This approach is more comprehensive than the first method; that is, the approach works toward identifying the goals, which helps the analysts to be more focused.

Creating a goal tree that is useful for analysis can be challenging. However, a project that documents system user intent and activities as a part of requirement elicitation helps in creating a goal tree. In case study 1, the flow of activities is captured using the contextual design sequence model [Beyer 1998]. The goal can be easily derived from the intent of each activity in the model.

8 Summary and Future Plans

In this report we have described the application of several privacy risk assessment approaches to two actual case study projects. We started with definitions of privacy and a survey of privacy risk assessment methods. We then discussed a way to classify the risk assessment methods, followed by classification of the methods. We selected two risk assessment methods, Privacy Risk Analysis for Ubiquitous Computing and STRAP, to apply to the case studies. For each case study we reflected on the results of the analysis. Neither approach was ideal, suggesting that perhaps a different approach or combination of approaches is needed to get maximum benefit. This will be considered as we move forward in the research.

This work is one of the activities that we have undertaken to extend SQUARE to include privacy considerations (P-SQUARE). We plan to continue our privacy risk assessment experiments and also to revisit other SQUARE steps to see what modifications are needed for privacy.

References

[Alberts 2001]
Alberts, C. J., Dorofee, A. J., & Allen, J. H. *OCTAVE Catalog of Practices, Version 2.0* (CMU/SEI-2001-TR-020). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/publications/documents/01.reports/01tr020.html

[Altman 1984]
Altman, Irwin & Chemers, Martin M. *Culture and Environment.* Cambridge University Press, 1984.

[AskOxford]
AskOxford. "Privacy." http://www.askoxford.com/results/?view=dev_dict&field-12668446=privacy

[Boehm 1991]
Boehm, B. W. "Software Risk Management: Principles and Practices." *IEEE Software 8*, 1 (Jan. 1991): 32–41.

[Bellotti 1993]
Bellotti, V. & Sellen, A. "Design for Privacy in Ubiquitous Computing Environments," 75–90. *Proceedings of the 1993 Third European Conference on Computer Supported Cooperative Work* (ECSCW 1993). http://www.ecscw.org/1993.htm

[Beyer 1998]
Beyer, H. & Holtzblatt, K. *Contextual Design: Defining Customer-Centered Systems*. San Francisco, CA: Morgan Kaufmann Publishers Inc., 1998 (ISBN: 1-55680-411-1).

[Buffett 2006]
Buffett, S. & Kosa, T. A. "Towards a Model for Risk and Consent Management of Private Health Information." National Research Council, Canada, 2006.

[Dardenne 1993]
Dardenne, A., Lamsweerde, A. V. and Fickas, S. "Goal Directed Requirements Acquisition." *Science of Computer Programming 20*, 1–2 (April 1993): 3–50.

[Divakaran 2009]
Divakaran, L., Inkook, S., & Lara, K. "How Significant Is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management." *Computers & Security 28*, 3–4 (May 2009): 215–228.

[Feinman 2000]
Feinman, J. M. *Law 101*. Oxford, England: Oxford University Press, 2000.

[Hand 1947]
United States v. Carroll Towing Co. 159 F.2d 169 (2d Cir. 1947).

[Hong 2004]
Hong, J. I., Ng, J.D., Lederer, S.D., & Landay, J.A. "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems," 91-100. *Proceeding of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques.* New York: ACM, 2004.

[IaChello 2005]
IaChello, G. & Abowd, G. D. "Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design in Ubiquitous Computing," 91-100. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM, 2005.

[IaChello 2008]
IaChello, G. & Abowd, G.D. "From Privacy Methods to Privacy Toolbox: Evaluation Shows that Heuristics are Complementary." *ACM Transactions on Computer-Human Interaction 15*, 2 (July 2008).

[Jensen 2005]
Jensen, C. & Potts, C. *Designing for Privacy in Interactive Systems*, Georgia Institute of Technology, Atlanta, GA, 2005.

[Jensen 2007]
Jensen, C. & Potts, C. "Experimental Evaluation of a Lightweight Method for Augmenting Requirements Analysis," 49-54. *Proceedings of the 1st ACM International Workshop on Empirical Assessment of Software Engineering Languages and Technologies*. New York: ACM, 2007.

[John 1996]
John, B. E. & Kieras, D. E. "The GOMS Family of User Interface Analysis Techniques: Comparison and Contrast." *ACM Transactions on Computer-Human Interaction 3*, 4: 320–351.

[Lederer 2003]
Lederer, S., Hong, J. I., Dey, A. K., & Landay, J.A. "Personal Privacy through Understanding and Action: Five Pitfalls for Designers." *Personal and Ubiquitous Computing 8*, 8 (2003): 440-454.

[Mead 2005]
Mead, N. R.; Hough, E.; & Stehney, T. Security Quality Requirements Engineering (SQUARE) Methodology (CMU/SEI-2005-TR-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.
http://www.sei.cmu.edu/publications/documents/05.reports/05tr009.html

[Merriam-Webster]
Merriam-Webster Online Dictionary. "privacy."
http://www.meriam-webster.com/dictionary/privacy

[Microsoft 2008]
Microsoft Corp. *Privacy Guidelines for Developing Software Products and Services*, Version 3.1, September, 2008. Available on the Microsoft Download Center,
http://www.microsoft.com/downloads/en/default.aspx.

[Microsoft 2009a]
Microsoft Corp. "Appendix C: SDL Privacy Questionnaire." Microsoft Developer Network, 2009. http://msdn.microsoft.com/en-us/library/cc307393.aspx

[Microsoft 2009b]
Microsoft Corp. *Microsoft Security Development Lifecycle (SDL) - Process Guidance*. Microsoft Developer Network, 2009.
http://msdn.microsoft.com/en-us/library/84aed186-1d75-4366-8e61-8d258746bopq.aspx

[Miyazaki 2008a]
Miyazaki, Seiya. "Compuer-Aided Privacy Requirements Elicitation Technique." MS thesis, Carnegie Mellon University, 2008.

[Miyazaki 2008b]
Miyazaki, S., Mead, N. R., & Zhan, J. "Computer-Aided Privacy Requirements Elicitation Technique," 367-372. *2008 IEEE Asia-Pacific Services Computing Conference*, 2008. Los Alamitos, CA: IEEE Computer Society Press, 2008.

[OPC 2006]
Office of the Privacy Commissioner. *Privacy Impact Assessment Guide.* Australian Government, 2006. http://www.privacy.gov.au/publications/index.html

[Palen 2003]
Palen, L. & Dourish, P. "Unpacking 'Privacy' for a Networked World," 1229-136. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM, 2003.

[Samuel 1890]
Samuel, W., and L. D. Brandeis. "The Right to Privacy." *Harvard Law Review* 3 (1890): 193.

[TBCS 2002]
Treasury Board of Canada Secretariat. *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, v2.0, August 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld-eng.asp

[Turkington 1990]
Turkington, R. C. "Legacy of Waren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Information Privacy." *Northern Illinois University Law Review 10*, 3, pp.479-482.

[University of California 1992]
University of California. *RMP-8, Legal Requirements on Privacy of and Access to Information.*
http://www.ucop.edu/ucophome/policies/bfb/rmp8.html

[Wikipedia]
Wikipedia. "Privacy." http://en.wikipedia.org/wiki/Privacy

[Woody 2006]
Woody, C., Coleman, J., Fancher, M., Myers, C., & Young, L. *Applying OCTAVE: Practitioners Report* (CMU/SEI-2006-TN-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/publications/documents/06.reports/06tn010.html

[Yassine 2008]
Yassine, A. & Shirmohammadi, S. "Privacy and the Market for Private Data: A Negotiation Model to Capitalize on Private Data," 669-678. *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications.* Los Alamitos, CA: IEEE Computer Society Press, 2008.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	July 2009	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Privacy Risk Assessment Case Studies in Support of SQUARE	FA8721-05-C-0003

6. AUTHOR(S)

Varokas Panusuwan, Prashanth Batlagundu; Nancy Mead, Faculty Advisor

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2009-SR-017

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report contributes to further development of the Security Quality Requirements Engineering (SQUARE) method to address privacy. Risk assessment is Step 4 in the standard SQUARE process. This report examines privacy definitions, privacy regulations, and risk assessment techniques for privacy. The risk assessment techniques are classified using a standard method, and promising techniques are applied to two case studies. The case study results are provided along with future plans for SQUARE for Privacy.

14. SUBJECT TERMS	15. NUMBER OF PAGES
requirements engineering, requirements elicitation, security requirements, system security, SQUARE, case study, privacy, risk assessment	45

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL