Privacy Patterns for Online Interactions

Sasha Romanosky, Alessandro Acquisti
Heinz School of Public Policy and Management, Carnegie Mellon University
[sromanos, acquisti]@andrew.cmu.edu

Jason Hong, Lorrie Faith Cranor
School of Computer Science, Carnegie Mellon University
[jasonh, lorrie]@cs.cmu.edu

Batya Friedman
The Information School, University of Washington
batya@u.washington.edu

ABSTRACT

A proper security architecture is an essential part of implementing robust and reliable networked applications. Security patterns have shown how *reoccurring* problems can be best solved with *proven* solutions. However, while they are critical for ensuring the confidentiality, integrity and availability of computing systems, security patterns do not specifically (or necessarily) address the privacy of individuals. Building on existing privacy pattern work, we identify three privacy patterns for web-based activity: INFORMED CONSENT FOR WEB-BASED TRANSACTIONS, MASKED ONLINE TRAFFIC, and MINIMAL INFORMATION ASYMMETRY. The first pattern addresses a system architecture issue and draws on Friedman's model for informed consent. The second and third patterns provide support for end users and extend Jiang's 'Principle of Minimum Asymmetry.' These patterns describe how users can protect their privacy by both revealing less about themselves, and acquiring more information from the party with whom they are communicating.

Keywords

Privacy patterns, security, asymmetric information, signaling, informed consent.

1. INTRODUCTION

In 1997, Yoder and Baraclow introduced Patterns to the information security community [1]. Other researchers were inspired and developed additional security patterns [2], [3], [4], [5]. While these patterns provide solutions to information technology (IT) security infrastructure problems, they do not address the growing privacy issues that individuals face today. With online personal privacy becoming a major concern, commercial organizations and governments are being called to react by implementing appropriate security controls and policies. These problems have increased because of the following economic and social forces [12]:

- **More data exists**: The increased adoption and speed of technology enables massive forms of data collection and mining across disparate data sources. Also, the costs of recording user activity and data is so low that more government and commercial enterprises are able to keep more digital records for longer.
- **Re-identification is easier**: With the increased capabilities of both attackers and researchers, user re-identification is more feasible across more kinds of data.

- **Rewards are greater**: With more data at their disposal, and better ways of correlating it, attackers are finding more opportunities to exploit the data for financial gain.
- **More information is being made publicly available**: The US Freedom of Information Act combined with e-government initiatives and pressure for public and private organizations to make their data available presents a continuing source of data for both researchers and attackers.

This paper describes three situations where the privacy of an individual can be jeopardized by interacting online. We use "interacting" in the general sense where a user could be purchasing a product on an ecommerce website, sending an email across the public Internet, or simply accessing a public webpage. In all cases, the user is initiating a request for internet-based services, whether it is web, email, instant messaging, VOIP, or other form of communication. The three patterns presented are:

Pattern 1: INFORMED CONSENT FOR WEB-BASED TRANSACTIONS
Pattern 2: MASKED ONLINE TRAFFIC
Pattern 3: MINIMAL INFORMATION ASYMMETRY

The first pattern is a design pattern while the second and third patterns are user patterns. The first pattern draws on Friedman's and her colleagues' model for informed consent [10], [11] and has been adapted to web-based transactions. The second and third patterns build on Jiang's et al. work by extending their 'Principle of Minimum Asymmetry' [16]. This principle provides what are, in effect, two proven solutions for reducing information asymmetry:

- Decreasing the flow of information from the data owner (the user) to the data collector (the website). This is reflected in the second pattern, MASKED ONLINE TRAFFIC.
- Increasing the flow of information from data collectors to data owners. This is reflected in the third pattern, MINIMAL INFORMATION ASYMMETRY.

While the second and third patterns are written to help users protect their privacy, designers of privacy-aware systems may also benefit by implementing the solutions presented here.

The template used here is a simplified version of the Pattern-Oriented Software Architecture (POSA[2]) outline as developed by Bushman et al. [13] and is described in Appendix A.

2. RELATED WORK

2.1. Security Patterns

Many security patterns have been written to address enterprise, architectural and user-level security [1], [2], [3], [4] [5]. For example, the SINGLE ACCESS POINT [1] pattern describes a system where all access requests must pass through a single monitor. This becomes the only way to access the system, and no requests can bypass this control. The CHECK POINT [1] pattern then shows how requests can be authenticated, logged, and monitored. SECURITY SESSION [3] and FRONT DOOR [3] further extend this pattern language to provide both a single and *central* point for system authentication. SINGLE ACCESS POINT and CHECK POINT have been used countless times to provide access to operating systems, ecommerce websites, web-based portals and distributed software applications. SECURITY SESSION and FRONT DOOR form the basis for single sign-on applications such as Microsoft's .NET

[2] The POSA format was originally developed for software engineering patterns and so also describes other sections such as Dynamics, Implementation and Variations that we will not cover in this paper.

framework, federated identity management such as SAML[3] and numerous enterprise authentication solutions.

DMZ, PROXY-BASED FIREWALL, PACKET FILTER FIREWALL and ROLE-BASED ACCESS CONTROL [3] are other patterns with proven solutions that have become indispensable components of network and application security architectures.

2.2. Privacy Patterns

Security standards such as the Common Criteria [6] have been developed by security professionals and represent best practices that address many information security problems, including privacy. Schumacher mines the Common Criteria for privacy patterns and identifies PROTECTION AGAINST COOKIES and PSEUDONYMOUS EMAIL [7]. PROTECTION AGAINST COOKIES describes how a user can configure their web client to control how and when cookies are set and used. PSEUDONYMOUS EMAIL describes how internet users can send email without revealing their online identity. By mining for patterns in this fashion, the patterns revealed will necessarily be user-focused. That is, they will inherently provide solutions to problems faced by users of security hardware and software.

Chung et al., on the other hand, describe traditional design patterns [8]. They identified 45 patterns for the design in ubiquitous computing environments, 15 of which focused on privacy. They first selected a large number of possible patterns from their collective experience in human computer interaction and iterated through many rounds of testing and review. Then they performed a user study and demonstrated how the application of their privacy patterns accelerated the development process to produce a better overall design.

Sadicoff et al. describe a privacy proxy that helps inform users of a website's privacy practices [29]. It translates machine-readable privacy polices into a form recognized by humans and could be used to communicate the elements six elements of informed consent presented in this paper.

Schümmer introduces six patterns that could be grouped into 2 categories: patterns that block personal information from being transmitted to another entity, and patterns that filter information sent from others to the user [9]. The former set, specifically the MASQUERADE pattern, is most related to personal privacy in that it describes a system to control how much private information one chooses to reveal when interacting with others. The context of Schümmer's pattern language refers to physical interactions with others, whereas the patterns presented here refer to online interactions between a user and, typically, a remote computing system. Also, we address the privacy implications of information asymmetry in online interactions. That is, the balance of information between two parties and how an unbalance can affect a user's personal privacy.

In the context of this paper, we consider the term 'privacy' to be the amount of control (or lack thereof) that one has over one's personal information.

3. INFORMED CONSENT FOR WEB-BASED TRANSACTIONS

This pattern describes how websites can inform users whenever they intend to collect and use an individual's personal information.

[3] Security Assertion Markup Language is an xml standard for exchanging authentication and authorization information.

Although this pattern includes elements of a user interface design, it speaks more deeply than the interaction between a consumer and website and the sort of infrastructure that is needed to support the informed consent interaction model. A user interface would define the surface of the interface, such as how the interface should look and how content should be phrased. The user interface is just a part (but alone not sufficient) of a properly functioning consent form. In addition, well designed user interfaces are also an important part of fostering a website's credibility and may affect the extent to which a user chooses to disclose private information. However, that is beyond the scope of this pattern.

This privacy pattern focuses on user consent and information relegation. The principles described here are meant to help designers determine their design goals when communicating with users or collecting their information. These goals do not necessarily have to be highly technical or full of legalese. For example, they may simply include text next to e-mail subscriptions such as, "we will not sell or share your email under any circumstances." This pattern will, therefore, also help users understand the consequences of disclosing identifiable information once completing a transaction.

3.1. Context

Web developers and website interaction designers are creating a website that will collect personal information from users for a survey, registration, or other purpose. The organization may be motivated to protect the privacy of its users either because of legislative requirements such as HIPAA[4] or COPPA[5] or because of consumer market pressures.

3.2. Problem

To facilitate transactions, websites often use cookies to track users and web forms to collect personal information. However, users are often resistant to disclosing personal information because they are uncertain if it will be used without their consent or against their interests. The problem is: How can website designers communicate their intended uses for the information they collect from users?[6]

As website owners and designers, you must balance the following forces:

- You realize users want to visit your website and participate in its services without fear of unnecessarily being tracked and identified
- You realize users want to maintain as much control over their personal information as possible
- You have the right to request and use information and to refuse service to users who don't provide their information (except as restricted by law)[7]
- You are able to provide richer and more customized services when you know who your users are
- You know you must protect your users' privacy but you want to do so while minimizing your cost

[4] Health Insurance Portability Accountability Act is a US legislation created to protect the privacy of personal health information.

[5] Children's Online Privacy Protection Act is US legislation that governs the collection of personal information of children under the age of 13.

[6] While we recognize that some work has shown that individuals do not always act in their own best interests [14], for the purpose of this paper, we will assume they do.

[7] Some countries have laws that place restrictions on the types of information that may be collected, how it may be used, and the ability of companies to deny service to individuals who refuse to provide some information.

3.3. Solution

To the extent possible given the limits imposed by web technology, provide the user with the following six elements of informed consent: disclosure, agreement, comprehension, voluntariness, competence, and minimal distraction.

Disclosure: If you are either implicitly or explicitly[8] collecting identifiable data from a user, fully disclose how that data will be used and for how long. Also, clearly inform users of the practical risks and benefits of participating in the online interaction such as having the information sent to 3rd parties for marketing or research purposes.

Place disclosure information both on pages that are easily accessible throughout the website and particularly at the point of data collection as this is where it is most relevant. Providing easy access to this privacy policy will allow the user to form a decision before committing to the transaction.

Where important fields of data are requested, provide clear indication to the user as to why the data is required and how they will be used.

Agreement: Provide the user with the ability to opt-out of the agreement at any time. This would allow them to cancel any marketing or incentive solicitations, and prevent further information from being used by 3rd parties.

If an opt-in feature is used (for example, for extra marketing incentives), setting the default value of "yes" or "checked" will typically produce greater positive results as people who are rushed or accept all default values will not change the options. However, this may reduce the voluntariness of the agreement.

Comprehension: To the extent possible, ensure that the user understands how the information that is being requested of them will be used. That is, confirm that the user realizes the liabilities and benefits. E.g., does the user know what a "cookie" is? Does the user understand when or if the data will be deleted? Who can have access to the date and for what purposes? Users may see the text of a privacy policy, but have they read it and do they know what it means?

Voluntariness: Ensure as best you can, that the information is being offered without coercion or external influence by:

- Not manipulating the options so as to suggest a certain course of action. E.g. suggesting that users can only enjoy special services if they register on the website.
- Not manipulating the options so as to mask useful or necessary of information (contributing to information asymmetry). E.g. hiding the privacy policy.
- Offering alternate means of fulfilling the service to users if they feel uncomfortable with the current method. This may be an online chat service, phone number to access a live customer service representative, fax service or standard postal mail.

Competence: To the extent possible ensure that the user from whom you are soliciting information is adequately competent to provide that information. For example, ensure that the user is of legal age. A commonly used (but not foolproof) practice is asking the user to submit their birth date during the registration process.

[8] An example of implicit collection would be through cookies, or logging of client IP address. Explicitly would refer to directly asking a user for their information (e.g. when registering for a website).

Minimal Distraction: Provide each of these functions without significant diversion from the service that you are providing. Not doing so would both cause frustration on the part of the user and likely result in fewer transactions.

One method for accomplishing this is to open a separate browser window that displays the relevant information, such as a clearly formatted privacy policy. Using a separate browser window allows the user to continue with the transaction (e.g. filling in a web form) without having to be directed away from the form, then back, forcing them to re-enter data.

3.4. Known Uses

This pattern is used in whole or part by many ecommerce, financial and health websites such as Yahoo!, Intuit, Google, and ehealthinsurance.com. For instance, the Yahoo! Email registration form, as shown in Figure 1, provides mouse-over dialogue boxes that inform the user about why certain fields (e.g. birthdates) must be filled out accurately.

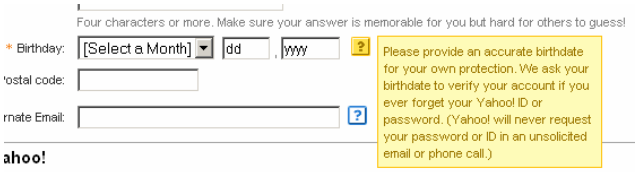

Figure 1: Yahoo! Registration Form

The Intuit registration form shown in Figure 2 discloses how they use the information and offers the option of opting-out of correspondences.

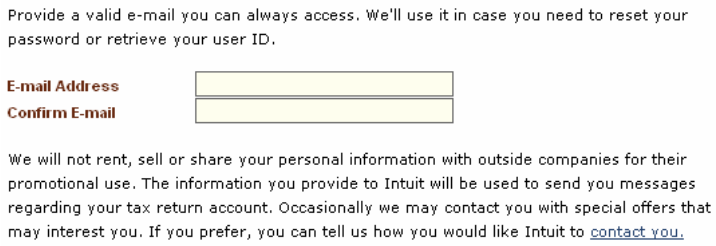

Figure 2: Intuit Registration Form

This pattern is consistent with the Fair Information Practices (FIP) recognized by many website policies and privacy laws[9] and is part of the standard practice for patient care established by the American Medical Association,[10] and U.S. Office for Human Research Protections (OHRP).[11,12]

Platform for Privacy Preferences (P3P) [15] is a computer-readable (and searchable) method used by websites to define and publish their policies for collecting and using information. The policies can be automatically read by user-agents to indicate whether or not the website's policies match a user's privacy preferences and helps provide both Disclosure and Minimal Distraction.

This pattern is also used by software developers of desktop applications who request that users provide personal information, or as a means for the application to collect usage data from the user.

[9] http://www.ftc.gov/reports/privacy2000/privacy2000.pdf
[10] http://www.ama-assn.org/ama/pub/category/4608.html
[11] http://www.hhs.gov/ohrp/humansubjects/guidance/ictips.htm
[12] EU Privacy Directive, http http://europa.eu.int/comm/justice_home/fsj/privacy/

This information is typically captured during installation or while using the application, and transmitted online to the software vendor.

3.5. Consequences

This pattern offers the following benefits:

- Helps to reduce information asymmetry between the user (data owner) and the website (data controller).
- Empowers users to make informed decision that do not conflict with their tolerance for private information disclosure.
- Provides a basis for trust between the consumer and website owner by establishing an expectation of practice by the website. Consider the risk of lost trust for ecommerce, medical and financial companies such as eBay, Amazon, Bank of America, ehealthinsurance.com, etc..
- This pattern can be applied to many other systems that interact with the user and external systems such as email and location aware devices (e.g. cellphones, PDAs).

This pattern suffers from the following liabilities:

- This pattern cannot provide any assurance that a website will comply with the informed consent model.
- Privacy policies are generally known to be confusing for the user to read and fully understand.
- The website may not wish to disclose their ability to track users without their knowledge.
- The website may not have the infrastructure to offer and support each of the solution elements for every user. For example, the ability for users to opt-out of the agreement.
- If the distraction due to implementing this pattern is sufficiently great, the user may simply cancel the transaction altogether [10].
- Information provided to gain consent is necessarily a) limited and b) manipulated by the site to obtain consent – this implies that the actual consequences of the revelation of personal information may remain unknown to the user.
- Smaller web-enabled devices such as cell phones and PDAs may not be able to support Minimal Distraction as easily as full featured web browsers.

4. MASKED ONLINE TRAFFIC

Communicating across a public and untrusted network can have negative consequences if you have a false expectation of privacy and your messages are intercepted. This pattern provides solutions to help users protect their privacy by reducing the amount of information that they disclose while interacting online.

4.1. Context

You want to interact online but don't want to reveal more information than necessary about yourself. You fear that doing so would compromise your personal privacy. You are aware of various technologies and protocols that claim to protect your privacy[13], but you are uncertain how and when to use them.

4.2. Problem

You are looking for ways to reduce the amount of personal information that you disclose, but you realize that you must eventually disclose some information in order to transact with the other party.

[13] Such as mixnets, onion routing and public key encryption

The problem is: How do you reduce the amount of personally identifiable information that is sent across a public network?

You must balance the following forces:

- You want to communicate with another entity, but maintain anonymity with respect to anyone listening on the channel, and possibly even with the receiver
- While the message itself may be unreadable by anyone, the mere act of communicating may reveal more information than you are comfortable with
- You shouldn't have to be a security or technology expert to hide your communication
- You want solutions that are convenient and easy to use

4.3. Solution

Employ *Anonymity Techniques*, *Blocked Requests* and *Privacy Behaviors* to mask or prevent identifiable information from being disclosed. These will limit the amount of information that can be collected and used without your consent. For example, as in product or price discrimination[14] [20]. In essence, there are two issues to consider. The first is sender anonymity. This refers to you, the sender, remaining unidentifiable to the party with whom you are communicating. The second issue is unlinkability and refers to the inability for anyone to determine that you are communicating with a particular receiver.

4.3.1. Anonymity Techniques

Employ techniques that prevent identifiable information to be transmitted, not only to the party with whom you are communicating, but to anyone who may be eavesdropping. For example, when researching or investigating online organizations you may want to remain fully anonymous up until the point where you decide to transact with them. Anonymizing systems ensure that you are completely unidentifiable to other parties whereas pseudonymous systems prevent you from being identified as an individual[15] but still enable communication between unique parties.

4.3.2. Blocked Requests

Websites often use cookies and web bugs[16] to track users, often without their consent or knowledge. Therefore, employ software tools and techniques that prevent other parties from tracking your online activities. PROTECTION AGAINST COOKIES [7] describes different methods for controlling how your web browser manages cookies. For example, blocking all cookies (though possibly at the expense of usability of some websites), or only accepting individual cookies. REASONABLE LEVEL OF CONTROL (C4) [8] recommends 'pushing' rather than 'pulling' data when communicating with others, giving you a greater level of control over how much and what kind of data is transmitted to others.

4.3.3. Privacy Behaviors

Adopt appropriate privacy behaviors that prevent unnecessary disclosure. PRIVACY ZONES (C8) [8] describes how risks to personal privacy can originate from the physical world just as well as the digital world. If your conversation is susceptible to human eavesdropping (from a computer monitor or VOIP phone conversation) move to an area where you cannot be overheard. BLUR PERSONAL DATA (C9) [8] recommends only providing as granular of information as is necessary and 'blurring' the rest. For example, provide regional (city or state) rather than specific location information.

[14] While this can benefit you as the consumer, it can also work against you.
[15] This is often done with aliases, or temporary user credentials
[16] http://www.eff.org/Privacy/Marketing/web_bug.html

These solutions can provide anonymity and privacy, however, they cannot prevent you from unnecessarily or inadvertently disclosing personal information (in a web form, or instant message, for example).

4.4. Known Uses

Anonymizer[17] offers both a free and commercial service that anonymously marshals web requests on your behalf. Note that it does not necessarily provide confidentiality because not all requests are sent encrypted. Anonymous proxies[18] are also free and publicly available but offer various degrees of anonymity.

Tor is a freely available application that implements the Onion Routing protocol [24]. Onion Routing employs a collection of routers that encapsulate a request within multiple layers of protection. Each node is aware only of the previous and subsequent hop, thus masking the true source and destination of the request [17]. It routes all traffic over the SOCKS[19] protocol through the onion network, thus providing confidentiality for any networked application that is configured to use it. For example, even an encrypted terminal session like SSH can be used in conjunction with Tor to provide confidential and anonymous communication. Of course, complete anonymity may not be possible if you need to authenticate to the SSH server.

Privoxy[20] is a software application that acts as a virtual proxy server to any web browser. It provides a range of services to assist with anonymous web browsing including blocking cookies and banner ads, and disabling client scripting. Web bugs are another form of traceable identifier that is used within web pages and html emails and can be blocked either by configuring the web browser to only load images from the originating server[21] or disabling html rendered email.

Pseudonymous remailers [7], [23] function as mail server relays that will substitute your real email address with a pseudonym. When a response is returned to the server, the pseudonym will be replaced by your actual email address and delivered to you. Examples of pseudonymous remailing can be seen with online services such as eBay, Craigslist[22], social network sites (e.g. dating) and in the Mixminion protocol [25].

When sending confidential files or emails, encryption features are often available and protect the secrecy of the message being transmitted. Note that these only protect the privacy of the message itself, not the source or destination of the message. PGP[23] is a software application that can encrypt both data files and email messages and the Trillian[24] and Off-the-Record[25] applications provide encryption for instant messaging clients.

People often retreat to private rooms in their home or office to engage in private conversations and use sunglasses and headwear to mask their identity – effectively reducing the amount of identifiable information they transmit to others.

---

[17] http://www.anonymizer.com/
[18] Such as http://www.stayinvisible.com/ and http://www.proxy4free.com/page1.html
[19] http://tor.eff.org/support.html.en
[20] http://www.privoxy.org/
[21] As is done with the Firefox web browser
[22] http://www.craigslist.org
[23] http://www.pgp.com/
[24] http://www.ceruleanstudios.com/
[25] http://www.cypherpunks.ca/otr/

4.5. Consequences

This pattern offers the following benefits:

- You are now able to communicate with another party while remaining fully anonymous.
- Used in conjunction with encryption (PGP) or encrypted channels (SSL), you are also able to achieve confidentiality of the message.
- The solutions offered do not require advanced knowledge of internet or security technologies, but only the basic ability to install and operate desktop software.

This pattern suffers from the following liabilities:

- Because some technologies are based on sophisticated security protocols, and complicated implementation they are susceptible to attacks[26] and abuses. For example, using an anonymizing proxy to marshal requests implies that the proxy is able to see, and therefore monitor your communication, thus negating any benefit.
- The Tor Onion Routing network can incur significant performance degradation because of the additional hops, sometimes to the point where you may stop using it.
- Transacting with certain websites (either purchasing products or logging into systems) may not be possible through anonymous communication.
- Anonymity can sometimes lead to "bad behavior" [26] in online social environments (chat rooms, message boards, etc).

5. MINIMAL INFORMATION ASYMMETRY

This pattern describes how you can protect your privacy by gathering more information about the parties whom you would like to transact online. By gathering more information, you are able to make more informed decisions and transact only with the parties you trust.

5.1. Context

You are an online consumer and want to interact with websites that sell products or services, register for their online services such as electronic banking, health insurance, or subscribe to local news and events. However, you are often disadvantaged by having less information about the products or services, or conditions of the agreement than does the website. Lacking sufficient information or the right kind of information may compromise your privacy either during the online transaction or because of the practices of the party you are dealing with. MASKED ONLINE TRAFFIC showed how your privacy could be protected by reducing the amount of information that you transmit to others. This solution represents the second (complementary) way to reduce the likelihood of privacy violations from information asymmetry

5.2. Problem

Information asymmetry is generally described as one party having more or better information about a transaction than the other. Unfortunately, in this context, the website generally has the better information. The problem is: How can you shift the balance of information in order to make a better decision when transacting online?

You want to resolve the following forces:

- You want to purchase products or services from an unknown party, and so you want to gather as much information about them as possible, before you disclose any information

[26] [18] provides an analysis of mix-nets and offers solutions to possible attacks

- You want to complete the transaction easily without having to account for (potentially) future detrimental consequences such as fraud or privacy violations
- You don't want to disclose more information than is necessary, but realize that in order to perform the transaction, you will have to disclose some identifiable information

5.3. Solution

Acquire more information by visiting websites that implement *Informed Consent* and *Signals*.

5.3.1. Informed Consent for Online Transactions

Visit websites that implement INFORMED CONSENT FOR WEB-BASED TRANSACTIONS. Organizations that properly implement the informed consent model provide you with more information about how your information will be collected and used. They may also provide you with the ability to opt-out (or opt-in) of their business services.

5.3.2. Signals

Signals are messages distributed by a website or third party that provide more information to you, as a current or potential consumer. Signals attest to the quality of the product or service offered by the website, or to the conditions of the purchase agreement. Where possible, recognize signals that shift the balance of information in your favor. Note that two conditions must exist for these signals to benefit you:

- The signal must be relevant: Being overloaded with irrelevant information may confuse and discourage you. For example, receiving unnecessary details about a product that aren't useful when comparing products.
- The signal must be credible: Signals can be good or bad, credible or not. Make sure you are acting on signals that originate from a known or trusted source. Signals that are less costly to produce or distribute will likely be less credible. For example a website simply claiming they are "The Best" is a cheap signal[27] and probably not as credible as rigorous third party analyses or benchmark testing.

Check for one or more of the following signals:

- Feedback mechanisms: Comments from past customers offer the advantage of real-world experience dealing with the site and the product. Instead of having to rely on the word of the website, or blind faith, you can make a more informed decision because other users can attest to the quality of a particular product or service.
- Reputation system: The reputation system enables customers to rate the service quality of other members within the community. This mechanism can be very effective when the ratings are publicly available.
- Warranties: Warranties are a way of certifying that the product or service matches prescribed standards for performance and quality.
- Money-back guarantees: This type of agreement assures you that if you are not satisfied with the product or service you will be reimbursed fully with little or no inconvenience.
- Privacy Policies: Read the privacy policies of websites to determine whether they meet your tolerance for privacy and confidentiality. The Privacy Bird[28] search tool can help find websites that match your privacy preferences.

[27] The notion of the value of a signal being a function of its cost is courtesy of the economist Michael Spence and his work on the effects of education and the labor market.
[28] http://search.privacybird.com

5.4. Known Uses

Many online organizations provide signals to their customers. Often they are publicly and freely available, but can also be purchased by third parties. The online auction site, eBay, for example, uses a reputation system to assist other buyers in feeling more comfortable purchasing from an unknown seller. Many other ecommerce sites (such as Amazon) rely heavily on the reputation and referral systems in order to help customers make a more informed decision.

Websites are more commonly publishing their privacy policies in order to assuage the privacy concerns of their users [19]. Users are also stating that they would be more comfortable interacting online if the site had displayed the TRUSTe[29] or BBBOnline[30] symbols, or had a privacy policy [21].

5.5. Consequences

This pattern offers the following benefits:

- You are able to reduce the risk of privacy violation by making more informed decisions regarding the websites you visit and the information you disclose.
- When information asymmetry is diminished, externalities (such as negative costs to you) can be minimized.
- Reduced information asymmetry can sometimes reduce inefficiencies in a market.[31]

This pattern suffers from the following liabilities:

- Some messaging systems that provide signals can be counter-productive. For example, newsgroups and message boards often create information overload and at times, provide unsubstantiated or erroneous information.

6. DISCUSSION

The solutions presented by these privacy patterns, just as with all patterns, seek to balance the forces that exist within the context of the problem. However, they may be unable to resolve all forces and will therefore result in a compromise between competing needs. For example, a financial cost may result from a certain technology that creates a more secure infrastructure. There may also be tradeoffs to convenience (customer usability, or system manageability) or complexity for a pattern that requires many separate components.

Eli Noam is quoted as saying, “Privacy is an interaction in which the information rights of different parties collide. The issue is of control over information flow by parties that have different preferences over ‘information permeability’” [27]. This statement wonderfully reflects the trade-offs made between two parties when interacting online. As we have attempted to show here, both users and websites must balance the amount of information that they are willing to provide while still satisfying their needs.

Software and security patterns have had the benefit of testing and refinement over many years, however privacy patterns (solutions), specifically, have not. We hope that the patterns presented here will contribute to the growing privacy pattern language and that both online organizations, website designers and users can employ them to ensure appropriate disclosure and use of personal information online.

[29] http://www.truste.org
[30] http://www.bbbonline.org
[31] As discussed in “The Market for Lemons” [28]

7. ACKNOWLEDGEMENTS

The authors would like to thank Markus Schumacher, Munawar Hafiz, Uwe Zdun and the PLoP 2006 workshop members for their helpful comments and suggestions.

8. APPENDIX A: PATTERN TEMPLATE

Name: The name provides a short descriptive title or active phrase that generally illustrates the solution.

Context: The context describes the general situations and assumptions under which the problem occurs. It describes the scope, market, user or other conditions that, if changed, would alter the problem or solution.

Problem: Describes the problem that repeatedly occurs and the forces that are in conflict for the given context. The forces can arise from tensions or conflicts from users, computing systems, corporations, the natural environment, legal regulations, etc..

Solution: This is the fundamental solution that best resolves and balances the forces. The better the forces are balanced, the better the solution. The discussion provides a guideline or strategy for implementing the solution and should allow the reader the freedom to craft the solution in the most appropriate way.

Known Uses: A true pattern will have many real-world implementations. Without these, the pattern is only a potentially great idea. The better a pattern can demonstrate actual uses, the better it is and the more useful it will be to others.

Consequences: Consequences describe both the benefits and liabilities of the pattern because solutions are not always able to resolve each of the forces. Therefore, any conflicts not resolved or limitations of the solution should be listed.

9. REFERENCES

[1] Joseph Yoder, Jeffrey Baraclow, “Architectural Patterns for Enabling Application Security,” Pattern Languages of Programs, 1997.

[2] Matjaz Juric, Nadia Nashi, Craig Berry, Meeraj Kunnumpurath, John Carnell, Sasha Romanosky, “J2EE Design Patterns Applied,” WROX Press, 2002.

[3] Markus Schumacher, Eduardo Fernandez, Duane Hybertson, Frank Buschmann, Peter Sommerlad (editors) “Security Patterns: Integrating Security and System Engineering,” Wiley Press, 2006.

[4] Bob Blakely, Craig Health, “Security Design Patterns,” The Open Group, 2004.

[5] Christopher Steel, Ramesh Nagappan, Ray Lai, “Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management,” Prentice Hall, 2005.

[6] International Standards Organisation, ”Common Criteria for Information Technology Security Evaluation” http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2, 1999.

[7] Markus Schumacher, “Security Patterns and Security Standards - With Selected Security Patterns for Anonymity and Privacy,” European Conference on Pattern Languages of Programs (EuroPLoP), 2002.

[8] Eric Chung, Jason Hong, et al., “Development and Evaluation of Emerging Design Patterns for Ubiquitous Computing,” Patterns C1-C15, DIS2004, 2004.

[9] Till Schümmer, “The Public Privacy – Patterns for Filtering Personal Information in Collaborative Systems”, CHI 2004.

[10] Batya Friedman, Lynette Millett, Edward Felten, “Informed consent online: A conceptual model and design principles,” UW CSE Technical Report 00-12-02. Seattle, WA: University of Washington, Department of Computer Science and Engineering, 2000.

[11] Batya Friedman, D.C. Howe, Edward Felten, “Informed consent in the Mozilla browser: Implementing Value-Sensitive Design,” proceedings of the Thirty-Fifth Annual Hawai'i International Conference on System Sciences, Abstract, p. 247; CD-ROM of full-paper, OSPE101. IEEE Computer Society: Los Alamitos, CA, 2002.

[12] George T. Duncan, Robert W. Pearson, “Enhancing Access to Microdata while Protecting Confidentiality: Prospects for the Future,” Statistical Science, Vol 6, No3, pp219-239, 1991.

[13] Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad, Michael Stal, “Pattern-Oriented Software Architecture,” John Wiley & Sons, 1996.

[14] Alessandro Acquisti, “Privacy in Electronic Commerce and the Economics of Immediate Gratification”, EC’04, 2004.

[15]Lorrie Faith Cranor, “Web Privacy with P3P,” O’Reilly Media Inc., 2002.

[16] Xiaodong Jiang, Jason Hong, James Landay, “Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing,” University of California Berkeley, 2002.

[17]David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, "Onion Routing for Anonymous and Private Internet Connections," Communications of the ACM, vol. 42, num. 2, February 1999.

[18] Andrei Serjantov, George Danezis, “Towards an Information Theoretic Metric for Anonymity” University of Cambridge, 2002.

[19] Serge Engelman, Lorrie Faith Cranor, Abdur Chowdury, “An analysis of P3P-Enabled web sites among Top-20 Search Results” Carnegie Mellon University, 2005.

[20] Andrew Odlyzko, “Privacy, Economics, and Price Discrimination” Digital Technology Center, University of Minnesota, 2003.

[21] Lorrie Cranor, Joseph Reagle, Mark Ackerman, “Beyond Concern: Understanding Net Users’ Attitudes About Online Privacy” AT&T Labs, 1999.

[22] Michael Reiter, Aviel Rubin, “Crowds: Anonymity for Web Transactions” Communications of the ACM, 1999.

[23]David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM , v. 24, n. 2, pp. 84-88, 1981.

[24] Roger Dingledine, Nick Mathewson, and Paul Syverson, “Tor: The Second-Generation Onion Router” Proceedings of the 13th USENIX Security Symposium, 2004.

[25] George Danezis, Roger Dingledine, Nick Mathewson. Mixminion: Design of a Type III Anonymous Remailer Protocol. IEEE Symposium on Security and Privacy, 2003.

[26] John P. Davis, “The Experience of ‘Bad’ Behavior in Online Social Spaces: A Survey of Online Users” Social Computing Group, Microsoft Research, 2002.

[27] Eli Noam, “Privacy and Self-Regulation: Markets for Electronic Privacy” Privacy and Self-Regulation in the Information Age, US Department of Commerce, 1997.

[28] George A. Akerlof, “The Market for Lemons: Quality uncertainty and the Market Mechanism” Quarterly Journal of Economics, 84(3), pp. 488-500, 1970.

[29] Mauricio Sadicoff, Maria M. Larrondo-Petrie, and Eduardo B. Fernandez, “Privacy-Aware Network Client Pattern” Proceedings of the Pattern Languages of Programs Conference, 2005.