2012 4th International Conference on Computer Engineering and Technology (ICCET 2012)
IPCSIT vol.40 (2012) © (2012) IACSIT Press, Singapore

A Framework Approach for Privacy in Socio-Technical Systems

Murthy V. Rallapalli

IBM/Stevens Institute of Technology Atlanta, GA, USA
e-mail: mr@us.ibm.com

Abstract. Information flows on Internet are vital to conducting business via Socio technical Systems (STS) in a global economy. Framework approach generally promotes a flexible approach to information privacy protection, while avoiding the creation of unnecessary barriers to information access. Internet technologies, particularly, e-commerce based businesses that link to the Internet and other information networks have made it possible to collect, store and access information from anywhere in the world. These technologies offer great potential for social and economic benefits for business, individuals and governments. However, while these technologies make it easier for consumers to shop with increased convenience, it can be difficult for individuals to retain a measure of control over their personal information. As a result, there may be harmful consequences that may arise from the misuse of their information. There is a need to promote and enforce a certifiable, ethical and trustworthy information practices in e-commerce environment to bolster the confidence of individuals and businesses. This paper addresses one approach of using privacy framework in STS to provide service providers to commit to certain privacy practices that could lessen the privacy liabilities. At the same time provide control to web users on collection of their personal information and how it is used.

Keywords: component; Privacy, Socio-Technical System, Framework, Privacy Framework, Negotiating Protocol

1 Introduction

Socio-technical system refers to the interrelatedness of social and technical aspects of a system. In fact, it is much more complex than mixture of people and technology. Many of the individual actors in STS are difficult to distinguish from each other because of their close inter-relationships.

According to ComputingCases.org, STS can include the following [1]:

Hardware: Mainframes, workstations, peripheral, connecting networks.

Software: Operating systems, utilities, application programs, specialized code.

Physical surroundings: Buildings also influence and embody social rules, and their design can affect the ways that a technology is used.

People: Individuals, groups, roles (support, training, management, line personnel, engineer, etc.), agencies.

Procedures: Both official and actual, management models, reporting relationships, documentation requirements, data flow, rules & norms.

Laws and regulations: These also are procedures like those above, but they carry special societal sanctions if the violators are caught. They might be laws regarding the protection of privacy, or regulations about the testing of chips in military use. These societal laws and regulations might be in conflict with internal procedures and rules.

Data and data structures: What data are collected, how they are archived, to whom they are made available, and the formats in which they are stored are all decisions that go into the design of a socio-technical system.

STS represent an interpretive process made possible by optimizing the "goodness of fit" between technology and human systems. According to Aldridge [10], multi-factor analysis suggests that by maximizing the degree of self-regulation, work group productivity and job satisfaction will be consistently higher. Thus, socio-technical systems create the organizational context for knowledge sharing, learning and innovation enabling work groups to think and learn collaboratively thereby, develop original work patterns, maintain flexibility and competitive advantage. However, like any other system, STS has its own privacy challenges when dealing with web user's personal information.

This paper proposes a Privacy framework approach to address privacy challenges in STS. This paper is organized in the following sections: Section 2 is a discussion on Privacy challenges in STS. Section 3 introduces the concept of privacy framework approach. Section 4 describes the value proposition of privacy framework approach. Section 5 includes conclusions and future work.

2 Privacy Challenges in STS

Privacy is a tricky concept to define, but its significance is never in doubt. Nissenbaum [2] finds threats to privacy from contemporary technology-based systems and practices that have the capacity to track people, and to analyze and disseminate their private information, thus putting one's privacy in danger.

As socio-technical systems networks evolve into the next generation single window of communication channels for the vast majority of web users, it is likely that users will become more sophisticated about demanding control of their personal information. Information technology, especially digital, has raised growing concerns over privacy of ordinary citizen web users in that the technology bears a potentially disruptive power that threatens to compromise the privacy of individuals. One of the features of a STS is the data collection of web users while transacting business online. For example, one cannot purchase a book without giving out certain private information. The data collected is supposedly used as per the privacy agreement provided by the service provider. But reading and understanding these agreements is not a straightforward process. For example, to use RealNetworks Inc.s RealPlayer to view videos or listen to presentations, users must read and agree to a hefty 11,495-word privacy statement. Microsoft Corporation's MSN requires that users sign off on a 6,000-word privacy statement [7].

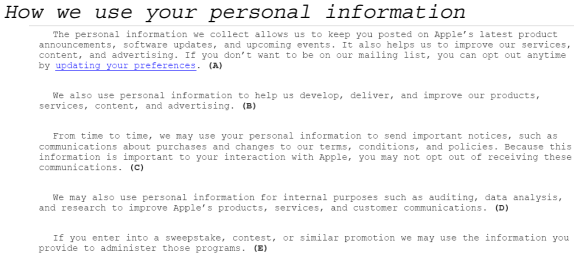
There is always a big question mark on the efficacy and legitimacy of privacy policies found on the Internet. There are also questions about whether web users understand privacy policies and whether they help consumers make more informed decisions. A 2007 study at the University of California, Berkeley found that "75% of consumers think as long as a site has a privacy policy it means it won't share data with third parties," confusing the existence of a privacy policy with extensive privacy protection [3].

Lack of awareness on web user's part given rise to monopolistic attitude on behalf of service providers on how to treat the web user privacy data. Two-thirds of people surveyed by the UK privacy watchdog want marketing opt-outs to be clearer, while 62% want a clearer explanation of how personal information will actually be used. The survey found that 71% did not read or understand privacy policies [4]. When the web users are not serious or care about their privacy data, there is little incentive for the service provider to tighten up privacy policies.

The fundamental purpose of a privacy policy is to disclose clearly the categories of information service providers collect, how collected information will be used, and with whom the information will be shared. The Federal Trade Commission (FTC) views a privacy policy almost like a contract with web users or web site visitors. If service providers promise certain activities or practices in privacy policy, but fail to deliver on a promise, the FTC says the business owners are liable for damages.

Table 1. Ten biggest data breaches in 2011 [12].

Organization	Breach Impact	Type of Data
SONY	101 million user accounts	Name, home, email addresses, login credentials, some credit card information
Epsilon	60 million email addresses	Email addresses and some names
HBGary Federal	60,000 records	Corporate emails, presentations, client reports
WordPress	18 million records	Source code, API keys, passwords
University of South Carolina	31,000 records	Names, addresses, health records, Financial data, and SSNs
TripAdvisor, Expedia	Unknown	User emails
RSA Security	Unknown	Information related SecureID technology
HuskyDirect.com, University of Connecticut	18,059 records	Names, addresses, credit card numbers, email addresses and phone numbers
Seacoast Radiology	231,400 records	Patient names, addresses, SSN and phone numbers
Ankle and Foot center of Tampa Bay	156,000	Names, Date of birth, Addresses, SSNs and Healthcare services received



How we use your personal information

The personal information we collect allows us to keep you posted on Apple's latest product announcements, software updates, and upcoming events. It also helps us to improve our services, content, and advertising. If you don't want to be on our mailing list, you can opt out anytime by updating your preferences. **(A)**

We also use personal information to help us develop, deliver, and improve our products, services, content, and advertising. **(B)**

From time to time, we may use your personal information to send important notices, such as communications about purchases and changes to our terms, conditions, and policies. Because this information is important to your interaction with Apple, you may not opt out of receiving these communications. **(C)**

We may also use personal information for internal purposes such as auditing, data analysis, and research to improve Apple's products, services, and customer communications. **(D)**

If you enter into a sweepstake, contest, or similar promotion we may use the information you provide to administer those programs. **(E)**

Figure 1. Apple's partial privacy policy on how it uses collected information.

A 2009 survey conducted by Ponemon Institute shows that organizations spent an average of $6.6 million per incident and more than $200 per compromised record [8]. According to Privacy Rights Clearinghouse website 542,214,290 data records were breached from 2,711 data beaches made public since 2005 [9]. Table 1 illustrates the ten biggest data breaches in 2011. These incidents highlight the dangers of putting personal sensitive data in the hands of profit-making business.

As long as there is no uniform standard for privacy agreements, making it easy to understand, they continue to come in various texts, sizes and ambiguous verbiage. The first step in standardizing privacy policies came from EU committee of data privacy commissioners, issuing guidelines to make corporate privacy statements easier to grasp and compare.

3 Privacy Framework Approach

The premise of this approach lies in the fact that a generic framework is feasible where in web users and service providers can negotiate privacy terms that are mutually agreeable. Once agreed, the enforcement is managed by a third party trusted agency thus relieving the service provider of huge responsibility of enforcing, what FTC terms as a legal contract.

In research terms, a conceptual framework is used to outline possible courses of action or to present a preferred approach to an idea or thought [5].

A Privacy framework is a set of collaborating services and capabilities that can be used as an analytical model for understanding and resolving security, trust and privacy related problems. It is extensible and designed to support regulatory-specific requirements across an array of industry cases [6].

To further discuss framework approach, let's take example of Apple's privacy policy. Apple, according to it privacy policy, uses collected information as shown in Fig. 1. To provide clarity and ease of reference the Fig 1. bullets are categorized from A thru E. Like any other privacy agreement presented to the web user there are only two choices included in Apple's privacy agreement as shown in Fig. 2. – 'Accept' or 'Decline'.

By presenting the dialog box as in Fig 2., the company is asking the question; You have the choice of either 'accept' or 'decline' how we are treating the information collected from you. In this scenario (Fig. 2), the web user either accepts A thru E (Fig. 1), or declines all of them without any middle ground.

In a framework approach, it provides an opportunity to negotiate privacy terms with the service provider's on its privacy terms. For example, the web user may choose to accept terms A and B, while declining terms C thru E. Once mutually agreed, it becomes incumbent upon service provider to maintain the terms. The framework can ensure that the terms are met to the mutual satisfaction of both the web user and service provider.

When a privacy agreement P contains sensitive information like Pa, Pb … Pn, where, P1..n are privacy terms A thru E in Fig. 1., then P itself requires a trusted protection in the form of an agreement for access to P. For example, a client interacting with an unfamiliar web service provider may request to see the exact privacy terms on Pa, Pb that attest to the server's handling of private information. This situation requires that trust be established through mutual negotiation on individual privacy constraints gradually leading to an agreed upon P, so that sensitive credentials are not disclosed to anyone outside of the defined P.

In this case, agreement Puser = f(A+, B+) & f(C-, D-, E-), implying, that the web user and the service provider have mutually agreed upon the privacy policies at a granular level. The P is then uniquely bound to the user (Puser) for all future interactions unless web user likes to renegotiate on future web interactions. The framework ensures that terms bound for the user with the agreement P is enforced.

In this approach, the privacy agreement and terms are unique to each user signing up the agreement. This provides benefits to both the web user and the service provider. For the web user, it provides better control of their privacy information. Web users can choose what terms are acceptable and they have a choice to negotiate on other terms as presented in the privacy agreement. Where as, for the service provider, it offers a unique opportunity to provide a meaningful privacy policy to its customers. In addition, since the enforcement is left to the framework, it relieves service providers of managing privacy data of web users. Using privacy terms negotiation, certified privacy practices can be represented in the form of digital

credentials or a predefined framework that can be disclosed in response to user policies that require certain privacy practice guarantees. By automating the privacy negotiation practices in a framework approach provides the service provider to commit to certain privacy practices that could lessen the privacy liabilities on data.

Violating privacy (intentionally or not) agreement can result in two significant problems to service providers: the loss of site visitors and the possibility of lawsuits. Breaking a privacy statement can have devastating effect on company's psyche and stock price. Following statistic is an indication of changing web user's attitude towards privacy [11]:

•77.5 percent think that privacy is more important than convenience

•71.5 percent think that there should be new laws to protect privacy on the Internet

•84.3 percent said that content providers shouldn't have the right to resell user information

•90.5 percent believe that users ought to have complete control of demographic information

4 Privacy Framework Value Proposition

The scope of the proposed framework is limited to Privacy and Trust in a web based socio technical system. The Privacy Framework is focused on providing a structure for the application of privacy principles in order to generate a baseline for assessment/audit capability in privacy policy management.

Web based STS applications which adopt the Privacy Framework have some incentive to do so (regulatory compliance, decreased liability, and risk minimization etc.). It may appear that the service provider has little motivation to participate in the privacy negotiation with the web user. On contrary, it is in their best interests to consider a negotiation process based on a framework. Privacy negotiations present the opportunity to develop a more systematic approach for handling web users' privacy data on the web thus reducing the unintentional misuse of privacy data collected from millions of web users. By automating the privacy negotiation practices in a framework approach provides the service provider to commit to certain privacy practices that could lessen the privacy liabilities on data.

5 Privacy Framework Implementation

Although the physical implementation details of the framework are left for the future research, this section discusses logical implementation.

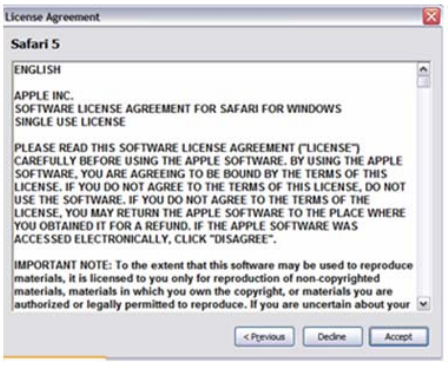


Figure 2. Apple's privacy policy with 'Decline' or 'Accept' choices.

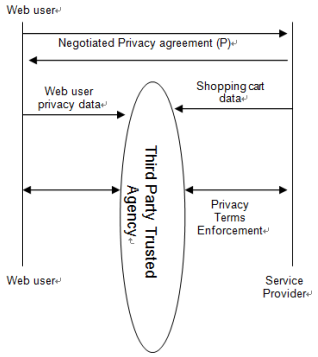


Figure 3. Logical implementation of privacy terms negotiation between service provider and a web user in a STS.

In the logical implementation scenario as shown in Fig. 3, a component called 'Third Party Trusted Agency' acts as a mediator between service provider and web user. This component facilitates the negotiation and mutual agreement of terms. This key component of the framework, trusted by both web users and service providers, provides the unique binding of privacy policy P with individual web users. In a physical implementation, this could be a web based agent that collects and stores the privacy data of the web users. This will alleviate the data storage responsibility from the service provider, allowing it to focus on fulfilling its core business requirements. There are several ways of physical implementation of Third party trusted agency that is left for the future research.

In this approach proposed model, the service provider has minimal responsibility of managing the privacy data, as it is managed by the Third party trusted agency. Upon completion of the privacy term, it is the Third party trusted agency that purges the data as per the privacy policy agreement between the service provider and the web user. There are big advantages in this model for the service provider. The service providers are relieved of any privacy liability risks from handling the web users' privacy data giving them the opportunity to focus more on fulfilling its core business rather than privacy management. For the web user, it is a definitive state that the privacy data is now out of the service provider's domain, handled by the third party trusted agency.

6 Conclusion

Clearly, data privacy is an important topic and each web site's information security system should enforce stated privacy policy. To provide a total privacy solution there are two actors that should work hand in hand; Privacy enhancing technology and privacy principled policies. Organizations leveraging STS should explore embedding privacy enhancing technologies such as privacy frameworks in their data privacy mechanisms to assure certified privacy practices in the form of digital credentials. This paper proposes two key privacy concepts – privacy terms negotiation framework and a trusted third party agency. Since privacy vulnerabilities exist when policy disclosures take place, the approach presented in this paper describes an environment to experiment with the proposed framework solution to the privacy problem in Socio-technical systems. This should lead to a more formal definition of a generic privacy framework adaptable by e-commerce websites with relative ease of use and in the process gaining web user confidence in privacy handling and increase in site usage.

7 Acknowledgment

Thanks for helpful discussions with Catherine Rickleman, e-learning architect at IBM, who patiently reviewed the paper for formatting as well as provided content suggestions.

8 References

[1] ComputingCases.org, "http://www.computingcases.org/general_tools/sia/socio_tech_system.html," 12/24/2011

[2] H. Nissenbaum, "PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE", STANFORD UNIVERSITY PRESS, 2010.

[3] Gorell, Robert. "Do Consumers Care About Online Privacy?" October, 2007. Grokdotcom.com citing to a study by Chris Hoofnagle, UC-Berkeley's Bolt School of Law. Samuelson Law, Technology & Public Policy Clinic, Berkeley.edu.

[4] OUT-LAW News, "Regulators demand clearer privacy policies", 2/16/2009, http://www.out-law.com//default.aspx?page=9795.

[5] Wikipedia.org, 1/25/2011, http://www.google.com/search?hl=en&defl=en&q=define:Conceptual+framework&sa=X&ei=inE_TdbpDYix8QPR2OTSBA&sqi=2&ved=0CBMQkAEs.

[6] ISTPA, 1/25/2011,http://www.istpa.org/faqs/framework.htm.

[7] Cameron Sturdevant, http://www.eweek.com/c/a/Security/Danger-Privacy-Agreements/, 2005-01-24.

[8] L. Ponemon Institute Research, 2010: http://www.ponemon.org/about-ponemon-research

[9] Chronology of Data Breaches Security Breaches 2005 – Present, http://www.privacyrights.org/data-breach , 10/9/2011

[10] John W. Aldridge, "Information on Socio-technical Systems," published in the Encyclopedia of Distributed Learning, ISBN 0-7619-2451-5, Sage Publications, 2004.

[11] GVU's 10th WWW User Survey, http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/, October, 1998

[12] eWeek.com, http://www.eweek.com/c/a/Security/10-Biggest-Data-Breaches-of-2011-So-Far-175567/, May 2011.