Trust Factors in Privacy Framework Enabled Socio-Technical Systems

Murthy Rallapalli

School of Systems & Enterprises, Stevens Institute of Technology / IBM, 955 Autumn Close, Alpharetta GA 30004, USA
mr@us.ibm.com

***Abstract*- A key part of efforts to improve consumer confidence to ensure the growth of electronic commerce requires a balance and promotion of an effective information privacy protection. The idea of a Socio-Technical System (STS) enabled by a Privacy framework to provide better privacy protection is often the focus of several privacy researchers. Given two types of similar STS where one is enabled by a Privacy framework, the other is not, how do web user's rate the sites in terms of privacy trust. This paper addresses and compares privacy trust factors between the two. Privacy Framework enabled websites act as an important tool in encouraging the development of appropriate information privacy protections. In addition, they provide a better way for individuals to retain a measure of control over their personal information. However, an end user is more concerned with the effective implementation of privacy policies by the service providers as presented in their privacy policies. This paper hypothesizes that *'Framework Enabled STS'* have increased information privacy protection than their counterparts that are not enabled by any privacy frameworks.**

Keywords- Privacy; Socio-Technical System; Privacy Framework; Privacy Framework Enabled Website

I. INTRODUCTION

A socio-technical system is a mixture of people and technology. In reality, it is a much more complex mixture. The term socio-technical system was coined in the 1960s by Eric Trist, Ken Bamforth and Fred Emery, who were working as consultants at the Tavistock Institute in London [1]. It is a system composed of technical and social subsystems. An example for this is a factory or a hospital where people are organized, e.g. in social systems like teams or departments, to do work for which they use technical systems like computers or x-ray machines [2]. A website enabling real time auctions by different actors online is also an example of a STS. Online collaborative tools are another kind of socio-technical space, where people may interact with each other, share information, exchange digital files, and collaborate. However, in each different use, the technology is embedded in a complex set of other technologies, physical surroundings, people, procedures, etc. that together make up the socio-technical system [3].

The lack of consumer trust and confidence in the privacy and security of online transactions in STS is one element that may prevent web users from gaining all of the benefits of electronic commerce. Ubiquitous access to e-commerce websites via mobile technologies, that seamlessly connect 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, and individuals, including increased consumer choice, market expansion, productivity, and faster access to the market. However, while these technologies make it easier to buy online, they also often make it more difficult for individuals to retain a measure of control over their personal information. As a result, there is a general concern about the harmful consequences that may arise from the misuse of their information. The Privacy framework enabled STS Websites, to some extent, to address this gap, by automating certain privacy practices and providing consistent and transparent data handling of web user's privacy data. Although the concept of framework enabled websites are at an early stage, it is a concept gaining traction and acceptance.

The dichotomy of above discussion leads us to two types of STS Websites:

1. Sites that collect privacy data using a Privacy Enabled Framework to govern and manage the privacy data. These types of STS Websites are referred to as Privacy Framework Enabled Websites (PFEW) in this paper.

2. Sites that collect privacy data but do not leverage any Privacy Enabled Framework to govern and manage the privacy data. Overwhelming majority of contemporary e-commerce based STS fall under this category. These websites are referred in this paper as 'Contemporary Websites'.

In the following sections, this paper will examine the privacy policies associated with both PFEW and Contemporary Websites. In addition to providing clear definition of each in logical architecture terms, it provides some empirical research data on trustworthiness of each type from the consumer point of view. Research discussion is around which type of STS provides a better trustworthiness and user control of privacy information, leading to the question of whether PFEW provides increased privacy protection of web user personal data.

This paper is organized in the following structure: Section 2 is a discussion on web consumers and data privacy; Section 3 provides a differentiation of PFEW and Contemporary Websites; Section 4 discusses Trust Factor Computations; Section 5 summarizes consumer data from various sources on consumer preference of shopping based on their privacy data protection; Section 6 includes conclusions and future work.

II. WEB CONSUMERS AND DATA PRIVACY

A 2002 report from the Stanford Persuasive Technology Lab contended that website's visual designs had more influence than the website's privacy policy when consumers assessed the website's credibility [4]. A 2007 study carried out by Carnegie Mellon University contends where privacy information is clearly presented, consumers prefer retailers who better protect their privacy and may "pay a premium to purchase from more privacy protective websites" [5]. Furthermore, 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 [6].

Lack of awareness on web user's part has 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 under-stand privacy policies [7]. 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 good news about dealing with consumer concerns about privacy is that policy statements on information use (how service providers utilize) have a very positive effect. In survey after survey, consumers report the same findings: "Show me a privacy policy statement, and I'll freely give you information" [8]:

•BCG Survey: 78 percent said privacy assurance would increase their comfort in providing personal information over the Internet.

•Harris/Westin Survey: 63 percent said they would have divulged information if the site disclosed clearly how the information would be used.

•NFO Interactive Survey: 69.4 percent of the 1,944 online consumers said they would purchase goods online if given assurance that their privacy was protected.

•AT&T Lab report: 84 percent of respondents said they would provide their ZIP code and answer questions about their interests in order to receive customized information if the data were confidential.

The above data support the arguments that as long as websites assure consumers that their privacy is protected, consumers are willing to return to STS. The Privacy Framework Enabled Websites (PFEW) attempts to provide certain degree of control to web users over their personal information.

III. PFEW VS. CONTEMPORARY STS

In a 'Contemporary Website', all the privacy data are collected upfront prior to making a sale. In this scenario, the vendor collects, stores, and governs the privacy data and assumes the liability associated with it. In some cases the vendor outsources the website management to third party hosts such as Yahoo or Google. Most small and medium sized e-commerce websites operating today follow this model.

A PFEW is a site which captures and channels the shopping cart data to fulfil the e-commerce request. For example, if a web consumer purchases a book online, the vendor's prime interest is fulfilling the order and collecting the funds. In addition, vendor would also be interested in collecting analytics for a better marketing. However, in the act of selling the book, vendor has to collect additional personal information. Personal information can be anything that can be used to identify an individual, not limited to but including; name, address, date of birth, marital status, contact information, ID issue and expiry date, financial records, credit information, medical history, where you travel, and intentions to acquire goods and services [9]. This is where the Framework adds value to the service provider's business model. While providing the e-commerce data such as quantity and product details to the vendor, the Framework collects and holds other privacy information within (disallows data sharing). Vendor can use a web service to retrieve private information such as address by using a unique transaction identifier. What this means to the vendor is that it does not need to worry about collecting and storing the privacy information, instead focuses on the core business of fulfilling the shopping cart. In this scenario, web users can actually negotiate with the service providers on the terms of their privacy information as shown in the Fig. 1.

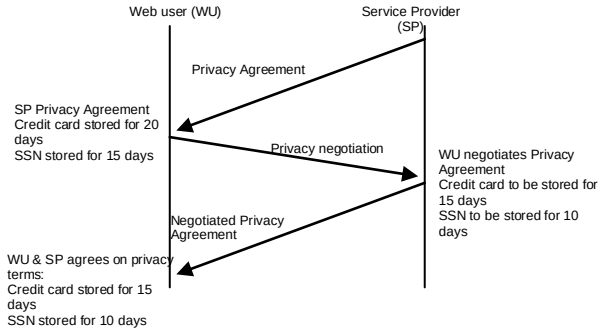

Fig. 1 Privacy Negotiation between a Service provider and Web user

In the Fig. 1, the service provider first displays the privacy agreement at the web user. The web user then chooses to negotiate the privacy terms provided in the privacy agreement. In theory, this negotiation can include several items of different domains, for the sake simplicity, this paper limits the scope to privacy terms such as Social Security Number (SSN) and Credit Card number. In the above example, service provider terms specify the intention of holding web user's credit card info for 15 days and SSN for 10 days after the transaction is executed.

There can be several legal, infrastructural, and technology reasons for service provider choosing the number of days. However, the web user, as shown in Fig. 1, may choose to negotiate to limit credit card data for 10 days and SSN for 5 days. Eventually, the service provider and the web user would reach an agreement. These agreed upon terms can then be part of the updated privacy agreement

presented to the web user for approval. If the web user and the ser-vice provider could not reach an agreement, then the web user has an option of declining the privacy agreement and not to go ahead with the transaction. Alternately, the web user may accept the privacy agreement provided by the service provider and go ahead with the transaction. The PFEW provides control over to web users on their privacy information, by directly negotiation their privacy terms with the service provider directly via the web site. In a broader sense, PFEW sites allow web users to control their privacy data by mutual negotiation with the service providers.

When a privacy agreement P contains sensitive information like Pa, Pb … Pn, where, P1..n are privacy terms such as credit card, SSN, Home address etc., 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.

IV. PRIVACY BREACHES DISMANTLE PRIVACY AGREEMENTS

Increasing number of data breaches is another reason for companies to adapt PFEW for their e-commerce revenues. Table 1 lists the ten biggest data breaches in 2011.

On February 20th, 2009, one of the largest payment card transaction processing companies in the United States reported a security breach. Information about the incident emerged slowly and few realized the magnitude and extent of the resulting impact. The final tallies proved shocking: over 100 million card accounts and 100,000 merchants impacted. The company's stock plunged by 75 percent within six weeks. Stunning as it may be, this incident is merely one in a growing trend of evermore sophisticated, continually ongoing data com-promises [10]. These are not one time data breaches either. Data breaches happen more often than reported in the press. With the advent of globalization, number of data breaches globally is increasing and global breaches are not systematically reported as they are in the U.S. Table 1 provides a partial list of all the data breaches in 2007. What these incidents indicate is that the privacy agreements provided by the service providers are not being strictly enforced either by accident or by negligence.

In spite of all these incidents, is there any real value to these privacy agreements in its current form? Why should I care that others know things about me? If it's true that some one has lousy credit, why hide the fact? It is not that people know things that impact anyone, rather based on this knowledge, what automatic decisions are made to judge people. Particularly, when these decisions are automated by a computer program that produces a judgment factor based on the data collected, the gap between the goal of data protection legislation and the reality of life in the society is not just a matter of poor technology implementation. It's a matter of judgment on web user on amount and type of data allowed to be collected online.

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 [11]. According to eWeek website, millions of data re-cords were breached in the first five months of 2011 alone [12]. These incidents highlight the dangers of trusting the privacy agreements and putting personal sensitive data in the hands of profit-making business.

TABLE 1 TEN BIGGEST DATA BREACHES IN 2011 [9]

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, adresses, 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

If a web site collects Fn privacy factors, where F represents privacy factors (such as SSN, Date of Birth) and 'n' represents the number of such privacy factors, it may allow negotiation of privacy factors by the web users. An example of negotiation is that the web user may mandate service provider not to hold to his/her SSN more than 100 days. Higher the value of 'n', better the trust worthiness of the web site as far as the web user is concerned. This requires two confirmation points:

1. Service provider provides an easier way to negotiate privacy data items;

2. Service provider provides an irrefutable proof of adhering the terms of the negotiation.

Sites enabled by PFEW can easily demonstrate not only the terms of the negotiation, but also confirmation when those terms are met. For example, if a web user negotiated SSN storage for 100 days, it is easy for the service provider to send a confirmation at the end of 100 days that the data has been purged from its data stores along with some kind of transaction identifier for future reference.

V. PFEW IMPLEMENTATION

While there can be several physical implementations, this section addresses one logical implementation. The

physical architecture is beyond the scope of this paper. However, with the emerging technologies in web servers, there can be several products and technologies that can be leveraged for physical implementation. The major difference between PFEW and Contemporary STS is that PFEW provides negotiation capability on privacy factors. The negotiation capability is provided by the underlying technology. An example of a typical privacy agreement in a 'Contemporary STS website' is shown in Fig. 2. It shows the options of 'Accept' or 'Decline' of the privacy agreement presented by the service provider.

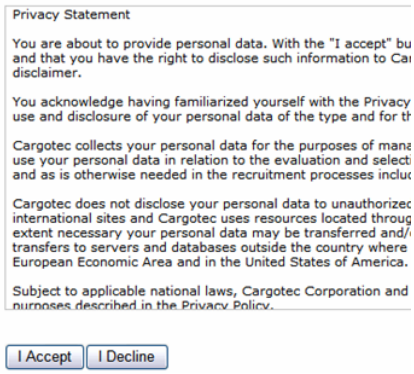

Fig. 2 Privacy Agreement Displayed by the Service Provider

As shown in Fig. 2, the web user can not proceed any further unless the privacy policy is accepted. The user has no choice but to accept privacy terms for any meaningful interaction. This gives little flexibility on web users' ability to influence how the service provider chooses to use the privacy data. This is the fundamental issue with the contemporary STS.

On the other hand, refer to the Fig. 3, which refers to a ST with PFEW enabled. In this case, the user has three options

Accept the privacy policy;

Decline the privacy policy, or;

Negotiate

It is this negotiation that empowers the web user to control what privacy data are being collected and how long the web user would like the service provider hold this information.

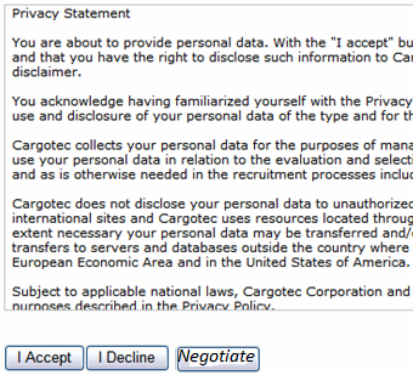

Fig. 3 Privacy Agreement Displayed by the Service Provider with an option to 'negotiate'

There are several privacy impacts with this model. While the web user is in control of what privacy information is being shared, there are also advantages to the service provider. It may appear that the service provider has little motivation to participate in the privacy negotiation with the web user. It is not only beneficial for the service provider; in reality it is in their best interests to consider a negotiation process. Privacy negotiations present the opportunity to develop a more systematic approach for handling web users' privacy data on the web. Using privacy constraints 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

VI. SUMMARY

Clearly, in STS, data privacy is an important topic and each STS site's information security system should enforce stated privacy policy. Organizations 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 a key privacy concept – privacy trust factors are higher in STS which are enabled by PFEW. This higher trust factors are attributed to the key concept of privacy negotiation ability provided to the web user. Since privacy vulnerabilities exist when policy disclosures take place, the approach presented in this paper describes an environment to experiment with the proposed model by negotiating the privacy problem. This should lead to a more formal definition of a generic privacy framework model adaptable by STS with relative ease of use. At this point, the physical implementation along with physical and logical architecture is left to future articles work efforts.

ACKNOWLEDGMENT

Author likes to thank Ms. Catherine Rickleman, e-learning architect at IBM, for helpful discussions with, who patiently reviewed the paper for formatting as well as providing content suggestions.

REFERENCES

[1] Socio-technical System, PRINCIPIA Wikipedia, http://en.wikipedia.org/wiki/Sociotechnical_system, Mar 15, 2012.

[2] Socio-technical System, PRINCIPIA CYBER-NETICA WEB, http://pespmc1.vub.ac.be/ASC/Socio-_Syste.html , Dec 17, 2011.

[3] Editorial Content (paragraph 2), Computing-Cases.org, http://computingcases.org/general_tools/sia/socio_tech_system.html ", Feb 1, 2012.

[4] Helen Nissenbaum, Privacy in Context: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE, STANFORD UNIVERSITY PRESS, 2010, 2006. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[5] L. Ponemon Institute Research Editorial

Report, http://www.ponemon.org/about-ponemon-research, 2010.

[6] 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)*FLEXChip Signal Processor (MC68175/D)*, Motorola, 2010.

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

[8] Bruce Spencer, "The effects of privacy policy statements on customer behavior", 12/13/1999J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 2008.

[9] McCormick, Michelle. "New Privacy Legislation." Beyond Numbers 427 (2003): 10-. ProQuest. Web. 27 Oct. 2011.

[10] Krista Tedder, "Don't Wait for a Data Compromise", January 2010, https://www.firstdata.com/downloads/thought-leadership/fd-data-compromise-wp.pdf.

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

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

Murthy V. Rallapalli is an Executive Architect in the area of Privacy and Security at IBM based in Atlanta, GA. He is a research scholar at Stevens Institute of Technology, Hoboken, New Jersey pursuing a PhD in the area of Privacy Frameworks and Socio-Technical Systems.

He authored a number of red books in the area of e-business and IT architectures. Published a number of research papers in privacy domain and holds two IBM patent submissions.