Technology and Investment, **2012, 3, 63-67**
http://dx.doi.org/10.4236/ti.2012.32009 Published Online May 2012 (http://www.SciRP.org/journal/ti)

Privacy Policies Considerations in Socio-Technical Systems

Murthy Rallapalli
Systems Engineering, IBM, Atlanta, USA
Email: mr@us.ibm.com

Received January 12, 2012; revised March 15, 2012; accepted March 23, 2012

ABSTRACT

The idea of a socio-technical system (STS) is an intellectual tool to help recognize patterns in the way technology is used and produced. Identification of these patterns will help in analyzing the ethical issues associated with the technology-and-its-social-system [1]. By way of example, consider a relatively simple technology: a set of twenty laptops connected by a local area network. The social and ethical issues associated with these networked devices will change dramatically depending upon the socio-technical system in which they are embedded. Few technologies have ever had the capability of gathering information (with or without the user's knowledge) as effectively as the World Wide Web. Internet has the greatest potential of targeting precise marketing demographics. Internet is also capable of disseminating information widely and quickly. This paper will study the role of privacy policies in web based socio-technical systems. This paper will research the role played by privacy policies in web user adaptation in the context of web based socio-technical systems.

Keywords: Privacy; Socio-Technical System; Framework; Privacy Framework; Negotiating Protocol; Web Services

1. Introduction

A socio-technical system is a mixture of people and technology. In reality, it is a much more complex mixture. It is a system composed of technical and social subsystems. 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 (Wikipedia). 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].

An STS is configurable—meaning that particular items in an STS can change or adjust in response to changes in functional or non functional requirements of systems over time [4]. For instance, an e-commerce website may introduce payments by a new device by Visa or Master- Card. But this change may also be reflected in changes in procedure and people. This paper assumes online web applications leveraged by web users as the context for STS.

While millions of web users leverage web based socio-technical systems, equal number privacy agreements are presented to the web users for their approval prior to proceeding any further on these systems. For example, one can not purchase and download a song on iTunes without agreeing to a three page privacy agreement (**Figure 1**).

In the following sections, this paper will examine the privacy policies associated with web based STS. This is the second in the series of three papers examining the

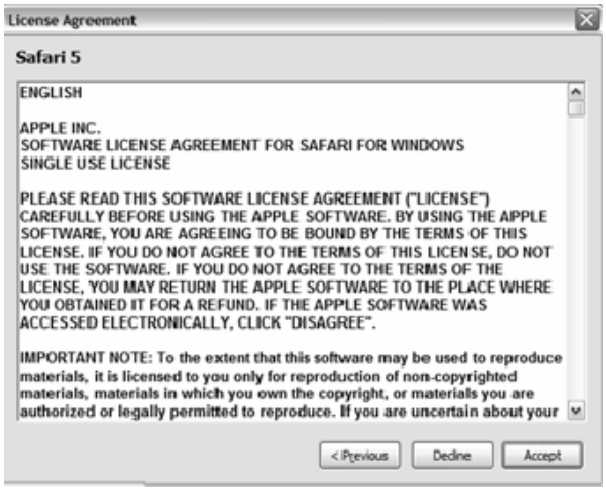

Figure 1. Privacy agreement by a service provider.

aspects of the privacy elements in STS. In addition to providing an overview of privacy policies, this paper examines real value it provides in its current form.

This paper is organized in the following: Section 2 is a discussion on web users & privacy agreements. Section 3 discusses the impact of privacy agreements on web users and service providers in typical STS. Section 4 describes various privacy agreements under the title "Not All Privacy Agreements are Created Equal". Section 5 includes conclusions and future work.

2. Web Users & Privacy Agreements

Privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data. 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 [5].

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 2002 report from the Stanford Persuasive Technology Lab contended that a website's visual designs had more influence than the website's privacy policy when consumers assessed the website's credibility [6]. A 2007 study 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" [7]. 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 [8].

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 [9]. 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.

Figure 1 is an example of a typical privacy agreement provided by service provider. Choices for the web user are limited to either "Accept" or "Decline". This indicates the upper hand the service provider has in dictating the privacy terms.

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" [10]:

- BCG Survey: 78% say privacy assurance will increase their comfort in providing personal information over the Internet.
- Harris/Westin Survey: 63% said they would have divulged information if the site disclosed clearly how the information would be used.
- NFO Interactive Survey: 69.4% of the 1944 online consumers say they would purchase goods online if given assurance that their privacy was protected.
- AT & T Lab Report: 84% of respondents said they would provide their ZIP code and answer questions about their interests in order to receive customized information if the data was confidential.

3. Effect of Privacy Agreements

3.1. Privacy Breaches Dismantle Privacy Agreements

Let's examine the following: "What value does privacy agreements provide to a web user?" Currently, it is the service provider who provides the terms of the privacy agreement including how privacy data of the web consumer is managed. Privacy breaches by many organizations are routinely reported in the media. A privacy breach involves improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information. These guidelines will focus primarily on the improper or unauthorized access to or disclosure of personal information as defined in the Privacy Act [11].

However, these service providers of trust are not foolproof as shown below:

Facebook has, in two separate instances, significantly abused the trust of its members by sharing personal information unilaterally without letting the members know in advance [12]. First, when Facebook started providing updates about changes in member profiles, and second, when it broadcasted members' purchases on other websites to their friends. Facebook is not alone in abusing the members' personal privacy data [13].

An April 13, 2001 article in the Wall Street Journal reported that profiling company ChoicePoint provided personal information to at least thirty-five government agencies [14]. The Federal Trade Commission (FTC) is conducting an investigation of ChoicePoint on the complaint of giving businesses, private investigators, and law

enforcement access to data that previously had been subjected to Fair Information Practices. In February 2005, ChoicePoint announced that the company sold personal information of at least 145,000 Americans to a criminal ring engaged in identity theft. California police have reported that the criminals used the ChoicePoint data to make unauthorized address changes on at least 750 people, and investigators believe that personal private information of up to 400,000 people in the United States may have been compromised [15].

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 compromises [16]. 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.

As socio-technical systems networks evolve into the next generation single window of communication channels for the vast majority of netizens, it's likely that users will become more sophisticated about demanding control of their personal information. 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. Information technology, especially digital, has raised growing concerns over privacy in that the technology bears a potentially disruptive power that threatens the social and political lives of individuals [17].

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 [18]. According to eWeek website millions of data records were breached in the first five months of 2011 alone [19]. These incidents highlight the dangers of trusting the privacy agreements and putting personal sensitive data in the hands of profit-making business.

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. Irrespective of how data gets exposed, the repercussions can be devastating to the web user when web user's privacy data is lost.

3.2. Privacy Agreements Are Not Created Equal

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

Table 1. Ten biggest data breaches in 2011.

Organization	Breach Impact	Type of Data Breached
SONY	101 million user accounts	Personal 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	Personal information including SSNs
TripAdvisor, Expedia	Unknown	User emails
RSA Security	Unknown	Information related SecureID technology
HuskyDirect.com, University of Connecticut	18,059 records	Personal Information
Seacoast Radiology	231,400 records	Patient names, addresses, SSN and phone numbers
Ankle and Foot center of Tampa Bay	156,000	Personal information including SSNs

FTC says the business owners are liable for damages.

Web users leveraging online services as part of their business digitally sign privacy agreements all the time. In the process, they are often agreeing to the installation of adware and spyware, not to mention setting the stage for increased spam. But reading and understanding these agreements is not a straightforward process. As an 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 6000-word privacy statement [20].

Other privacy agreements incorporate a generic wording "these guidelines are subject to change". For example, the privacy policy at the New York Times Web site (www.nytimes.com), for example, states: "These guidelines have been developed with the recognition that Internet technologies are rapidly evolving, and that underlying business models are still not established. Accordingly, guidelines are subject to change [21]."

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 EU committee of data privacy commissioners issued first ever formal guidelines to make corporate privacy statements easier to grasp and compare.

4. Privacy Agreement Implementation

Privacy statements are quickly becoming the cornerstones of e-commerce Web sites. These policy declarations are designed to quickly provide visitors with information on how personal data is secured, used and shared. In spite of the legal and regulatory focus on privacy declarations, only 65.7% of Web sites now include a privacy statement on their Web site [22]. For any web based retailer, small or big, a privacy policy statement is nothing less than a public legal document and a contract with the consumer. The main pitfall of any privacy statement is a failure to meet its policies as promised to the web user. A privacy statement breach occurs when a company expressly states that it will only use information in a particular situation (as explicitly mentioned in the agreement) and then does otherwise.

In August 1998, GeoCities settled with the Federal Trade Commission in the first case of privacy violation handled by the U.S. regulatory agency. GeoCities' violation consisted of misrepresenting the purpose for which it was collecting personal identifying information from children and adults. In this case, GeoCities lost both ways: The company had to pay for litigation, and the Web site reportedly lost 15% of its customer base as a result [23].

Breaking a privacy policy statement can result in two significant problems: the loss of site visitors and the possibility of lawsuits. Breaking a privacy statement can be so devastating. There are two likely forces that could influence the service provider's change in behavior in implementing privacy policies fully. The first is the threat of government and legal regulation if companies don't respond to consumer complaints about privacy online. But an even more potent force is the voice of consumers themselves. Adamant and privacy caring consumers can effectively bring change in service provider's privacy policy implementation. Following statistic is an indication of changing web user's attitude towards privacy [24]:

- 77.5% think that privacy is more important than convenience;
- 71.5% think that there should be new laws to protect privacy on the Internet;
- 84.3% said that content providers shouldn't have the right to resell user information;
- 90.5% believe that users ought to have complete control of demographic information.

5. Conclusion and Future Work

Good privacy agreements strengthen enterprises, but they're hard to find and careful scrutiny is needed. When people express concerns about privacy, it's about intrusion into personal affairs, disclosure of personal sensitive information, and judgments (functional judgments, not legal) based on data made available without consent. The more personal and sensitive information collected, the greater the reason for the above concerns.

There are choices to be made: should the privacy agreements follow certain formats that are easy to follow? If so, how should it be accomplished? What should happen to the information collected? Is the information collected is in tune with the privacy agreement presented? It is time to be more thoughtful about privacy agreements and their implications for privacy. Some of this thinking must happen among privacy advocates and technology implementers, and in addition, business and policy decision makers.

To provide transparency and consistency, future implementation may include privacy frameworks leveraging certified privacy practices represented in the form of digital credentials. By automating the privacy practices in a framework approach provides the service provider to commit to certain privacy practices that could lessen the privacy liabilities on data.

6. Acknowledgements

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

REFERENCES

[1] ComputingCases.Org, 2011. http://computingcases.org/general_tools/sia/socio_tech_system.html

[2] Principia Cybernetica Web, "Socio-Technical System," 2011. http://pespmc1.vub.ac.be/ASC/Socio-_Syste.html

[3] ComputingCases.Org, Editorial Content, 2012. http://computingcases.org/general_tools/sia/socio_tech_system.html

[4] ComputingCases.Org, Editorial Content, 2011. http://computingcases.org/general_tools/sia/socio_tech_system.html

[5] M. Michelle, "New Privacy Legislation," Beyond Numbers, 2003. http://www.ica.bc.ca/kb.php3?pageid=2326

[6] B. J. Fogg, "How Do People Evaluate a Web Site's Credibility?" 2002. http://www.nd.edu/~cclark2/capp30523/PDFs/HowDoPeopleEvaluate.pdf

[7] A. Alessandro, J. Tsai, S. Egelmana and L. Cranor, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," Carnegie Mellon University, Pittsburgh, 2007.

[8] G. Robert, "Do Consumers Care about Online Privacy?" 2007. http://www.mendeley.com/research/consumers-care-about-online-privacy/

[9] OUT-LAW News Editorial, "Regulators Demand Clearer Privacy Policies," 2009. http://www.out-law.com//default.aspx?page=9795

[10] B. Spencer, "The Effects of Privacy Policy Statements on Customer Behavior," 1999. http://www.techrepublic.com/article/the-effects-of-privacy-policy-statements-on-customer-behavior/5032632

[11] Treasury Board of Canada Secretariat, "Guidelines for Privacy Breaches," 2011. http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint-eng.asp

[12] A. Figueroa, "Privacy Issues Hit Facebook (Again)," 2010. http://www.pcworld.com/article/202315/privacy_concerns_hit_facebook_again.html

[13] N. O'Neill, "10 Privacy Settings Every Facebook User Should Know," 2009. http://www.allfacebook.com/facebook-privacy-2009-02

[14] Federal Trade Commission, "Choice Point Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress," 2006. http://www.ftc.gov/opa/2006/01/choicepoint.shtm

[15] Electronic Privacy Information Center, "Choice Point: Introduction and Background," 2001. http://epic.org/privacy/choicepoint/

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

[17] H. Nissenbaum, "Technology, Policy, and the Integrity of Social Life," Stanford University Press, Stanford, 2010.

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

[19] F. Y. Rashid, "IT Security & Network Security News & Reviews: 10 Biggest Data Breaches of 2011 So Far," 2011. http://www.eweek.com/c/a/Security/10-Biggest-Data-Breaches-of-2011-So-Far-175567/

[20] C. Sturdevant, "Danger: Privacy Agreements," 2012. http://www.pcmag.com/article2/0,2817,1752833,00.asp

[21] C. Sturdevant, "IT Security & Network Security News," 2005. http://www.eweek.com/c/a/Security/Danger-Privacy-Agreements/

[22] Second Moment, "Georgetown Internet Privacy Policy Survey," 2003. http://www.secondmoment.org/etal-column/georgetown.php

[23] http://www.ftc.gov/os/1998/9808/geo-cmpl.htm http://www.ftc.gov/os/1999/9902/9823015d&o.htm

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

