Chapter 3
Using Crowd Sourcing to Analyze Consumers' Response to Privacy Policies of Online Social Network and Financial Institutions at Micro Level

Shaikha Alduaij
University of Maryland, Baltimore County (UMBC), USA

Zhiyuan Chen
University of Maryland, Baltimore County (UMBC), USA

Aryya Gangopadhyay
University of Maryland, Baltimore County (UMBC), USA

ABSTRACT

As it becomes easy and inexpensive to store huge amount of data, concerns about privacy are increasing as well. Although service providers have privacy policies, research shows that users rarely read privacy policies. As a result, there has been little work done on how consumers respond to individual segments of privacy policies, which is important for organizations when designing privacy policies. In this study, the authors break down privacy policies of two well-known social network companies (Facebook, Twitter) and financial institution (Bank of America) into simple segments. They then use crowd sourcing to analyze consumers' response to these policy segments. The authors ask questions on users' awareness, expectations, familiarity, and privacy concerns of these policy segments. The relationships between various factors such as demographic factors, data type, data flow and consumers' privacy concerns were also investigated. The authors conclude with guidelines and suggestions for improvement and ways to increase users' awareness of privacy policies.

DOI: 10.4018/978-1-5225-7113-1.ch003

INTRODUCTION

The use of online services has become a necessity because it is involved in most individuals' daily activities, including those related to business, education, and communication. When using these services, users usually share their information for purposes such as registering a service, customizing their experience, or sharing their thoughts and interests with others. The collection and storage of this vast amount of information has raised users' concerns about how these practices will affect their information privacy. Natural questions arise in this context, such as how individuals' information will be stored, who will access it, how it will be used, and for what purposes.

To allay users' concerns, most of the service providers explain their practices with privacy policies. A privacy policy is a statement or legal document provided by the service provider to explain the handling of the users' gathered information by describing what information will be collected, how it will be used, with whom it will be shared, and the purpose of that sharing. Furthermore, it describes users' rights and options to change some of the practices.

It is important that a privacy policy is written and presented to user's clearly so they can understand how their information is being used. For example, Thelma Arnold, a user of the AOL search engine, did not know that AOL stored and shared her queries. Her identity was disclosed to the public by inferring her identity based on her queries. She stated in an interview, "My goodness, it's my whole personal life . . . I had no idea somebody was looking over my shoulder" (Barbaro & Zeller, 2006). Her unawareness of this practice could be because it was not clearly described in the AOL privacy policy or because she did not read the policy.

Making them clear and easy to understand would increase their readability and thus users' awareness of privacy practices. Some users accept the terms and conditions before using a service, and they are not aware of the risks that may be associated with the sharing of their personal data. The information users post or share online may be misused or used for purposes they are not aware of intentionally or accidentally. The risks or negative effect of using individual personal information can lead to embarrassment, decreased opportunity of employment, identity theft, cyber stalking, or phishing. These risks can happen by using information users themselves share without knowing how badly it can be misused. For example, some users may share on social media a photo for a ticket of an event they plan to attend. Any person who is allowed to view the picture may copy the barcode, print it, and use it (Ehling, 2013). Risks can also happen by using information stored in servers or shared with a third party. For example, an individual's identity may be associated with a disease when the information he searched for in a website is shared with third parties, disclosed to the public, or given to a data broker. This might affect users by loss of employment (Libert, 2015; Walters & Betz, 2012). Indeed, the availability of an individual's information can even lead to murder. Amy Boyer, a 20-year-old women from Nashua, was murdered after the criminal stalked her and gathered information about her work location using online sources (Donovan & Bernier, 2008).

Several research studies have tried to propose different solutions to improve privacy policies and increase users' privacy awareness. Some have introduced tools that help in privacy policy development and enforcement; others have introduced standardized presentations of privacy policies.

Research studies show that people think the privacy of their information is an important issue and they are concerned about it, but at the same time, they do not fully read the provided privacy policies for the services they use (Milne & Culnan, 2004). Some users believe that they do not have control over their information so they do not want to waste their time reading privacy policies if they are going to use the service anyway.