Chapter 5.11
Do You Know Where Your Data Is?
A Study of the Effect of Enforcement Strategies on Privacy Policies

Ian Reay
University of Alberta, Canada

Patricia Beatty
University of Alberta, Canada

Scott Dick
University of Alberta, Canada

James Miller
University of Alberta, Canada

ABSTRACT

Numerous countries around the world have enacted privacy-protection legislation, in an effort to protect their citizens and instill confidence in the valuable business-to-consumer E-commerce industry. These laws will be most effective if and when they establish a standard of practice that consumers can use as a guideline for the future behavior of e-commerce vendors. However, while privacy-protection laws share many similarities, the enforcement mechanisms supporting them vary hugely. Furthermore, it is unclear which (if any) of these mechanisms are effective in promoting a standard of practice that fits with the social norms of those countries. We present a large-scale empirical study of the role of legal enforcement in standardizing privacy protection on the Internet. Our study is based on an automated analysis of documents posted on the 100,000 most popular websites (as ranked by Alexa.com). We find that legal frameworks have had little success in creating standard practices for privacy-sensitive actions.

DOI: 10.4018/978-1-61350-323-2.ch5.11

INTRODUCTION

Business-to-consumer (B2C) electronic commerce is a vital part of the world economy. B2C sales in the USA were $138.6 billion in 2005 (Graumann & Neinert, 2006), $51 billion combined in Japan, South Korea, India and China in 2005 (Grau, 2007), and $87.8 billion combined in the UK, Germany, and France (the three largest B2C economies in Europe) in 2006 (Grau, 2006) (all figures USD). This vital industry is utterly dependent on the willingness of consumers to entrust sensitive personal and financial data to faceless online vendors. Conversely, distrust of websites and web services is a major deterrent to Internet use and e-commerce (Patil & Kobsa, 2009). A recent study by Consumer Web Watch reported that 86% of Internet users have changed their online behavior, while 29% have reduced their online purchases because of concerns about identity theft (Princeton Survey Research Associates International, 2005). A Pew Internet report (Fallows, 2004) found that although 75% of people thought that the Internet was a good place to conduct important transactions, only 55% had in fact done so—and then only to purchase low-value items such as concert or sports tickets. When the trust consumers have placed in a website is betrayed, the consequences can range from the merely annoying (telemarketing, differential pricing) to the financially crippling (identity theft).

We have previously argued (Reay, Dick, & Miller, 2009a) that the relationship between a consumer and a website contains a great deal of information asymmetry: the consumer has essentially no foreknowledge of how their private information might be utilized, while the website operator knows exactly what they intend to do with it (including holding the data for future uses). There is also a major inequality in power; the consumer *must* surrender their personal information to complete a transaction, but they cannot compel the website to use or refrain from using that information in any manner. In response to this inequality, the Organization for Economic Co-operation and Development long ago proposed a set of privacy-protection principles for the benefit of consumers (OECD, 1980). Today, websites will generally publish "privacy policies" on their websites, informing consumers of how their data will be used and their rights in relation to that data; the OECD privacy principles are the basis for the terms of these policies. In theory, at least, the OECD principles ought to form the basis of any standard of practice in online privacy protection.

A policy, however, is only a piece of paper; without external enforcement, it is meaningless. This "enforcement" takes many forms, and is dictated in part by the social norms of different countries. Thus, for instance, the United States has only enacted a hodgepodge of state and industry-specific privacy legislation, in keeping with the generally anti-government sentiment of U.S. society (Sun, 1994). Enforcement of those laws is not centralized in any one regulatory body; the Federal Communications Commission has the statutory authority to enforce a privacy policy once it is posted, but violations of other privacy legislation would fall under the purview of other agencies, or the states Attorneys-General. In the most general sense, "enforcement" in the United States is generally allowed to take the form of private litigation. European Union nations, on the other hand, have been far more willing to enact comprehensive privacy-protection laws, and the EU Data Protection Directive (European Commission, 1995) is the benchmark to which other privacy-protection legislation (e.g., Office of the Privacy Commissioner of Canada, 2000) and Japan (Government of Japan, 2003) is compared. These nations usually implement ombudsmen, registration offices, or licensing bureaus to enforce these laws; these are consolidated governmental enforcement mechanisms. Still other nations (notably Russia and China) have not enacted any privacy-protection legislation,