Chapter 1.38
The Desire for Privacy:
Insights into the Views and Nature of the Early Adopters of Privacy Services

Sarah Spiekermann
Humboldt University Berlin, Germany

ABSTRACT

Using privacy and security technology becomes increasingly important in many application areas for companies as well as for consumers. However, the market for privacy-enhancing technologies (PETs) is still small, especially in the private consumer segment. Due to the nature of the technology per se, little is known and can be learned about the views and motivation of those who carefully protect their transactions on the Net. Are they a niche group in the long run? Or do they hold views and have traits that promise a wider-spread adoption of PETs? This paper gives an insight into the traits and views of 5,037 customers of an anonymity service. Due to high service reputation and unchanged questions posted over 2½ years on the service's Web site, insights could be gained on PET users' demographic and psychographic traits. Moreover, 482 free-text comments provide a unique insight into the thoughts, feelings, and motivation for service usage.

INTRODUCTION

When we refer to anonymity and privacy today, we often refer to a right, for example, the "right to be let alone," as it was historically outlined by Warren and Brandeis (1890), or the "right to informational self-determination," as it is found in the German basic constitutional law. However, as electronic communication becomes ubiquitous, this right is increasingly being undermined. For those who want to protect their right, new tools and services are developed, maintained, and marketed: privacy-enhancing technologies (PETs).

One important PET is anonymizing technology. It is offered in such forms as anonymizing proxies, mixes, or onion routing procedures.

However, little insight has been gained into the users of privacy technology. Even though a long list of privacy studies have been conducted in past years showing that privacy and anonymity are a theoretic concern across countries and cultures, these studies have not treated the question of *why* people want to be anonymous[1]. Furthermore, there is only one study to our current knowledge, by Cranor, Arjula, and Guduru (2002), that has looked at the *actual* users of privacy technology. Knowledge on PET *usage reasons* and, thus, *motivation* to protect oneself in an electronic communication environment seem nonexistent as of today. Besides psychological investigations into the general desire for seclusion or self-disclosure (Cozby, 1973), no insight exists into the subject.

Consequently, researchers and developers in the area of PET technology, politicians, privacy rights organisations, and others have so far explained their efforts with the argument that privacy is inherent in our social heritage and must therefore be maintained. Equally, it has been assumed that the desire to be let alone is equally distributed across the population. Yet, increasing evidence from user behavior suggests that verbal concern may not fit in with peoples' actual behavior (Spiekermann, Grossklags, & Berendt, 2001). People pay little attention to the data traces they reveal and many do not know even about the existence of cookies. Of course, the fact that people know little about data collection and data deployment may be one explanatory factor for not protecting themselves. However, even those that are knowledgeable about technology often do not protect themselves. Consequently, more needs to be discovered about those who use (and buy) PETs. It should be investigated whether these early adopters are the forerunners of a bigger market. Are they different from the average Internet user and citizen? In what respect? And what reasons do anonymous surfers give for actively seeking protection? The current article sheds some light onto these questions. It does so by presenting results from a questionnaire-based study that was conducted over a time span of two and a half years with 5,037 users of a mix-based anonymity service called AN.ON.

METHOD

From July 4, 2001, to October 13, 2003, an online questionnaire was posted in German and English on the Web site of an anonymity service called AN.ON (http://anon.inf.tu-dresden.de). AN.ON is a free anonymity service with a client application called JAP. The service allows people to anonymously surf online. This means that neither Web servers nor a person's access provider, nor a malicious hacker can observe from whom and to whom Web page requests are being routed. AN.ON/JAP is technologically based on a mix infrastructure, operated mainly at public universities and institutions in Germany and the United States (New York). Currently, around 2,000 users are permanently online with the software and more than 20,000 people have downloaded the client application.

The Web-based questionnaire was answered by 5,604 service users from around the world during these two and a half years. For the current analysis, 4,896 answers originating from the German speaking territories and 141 answers from the United States were taken into account. For the German speaking territories, more precisely, 4,492 are from Germany, 194 from Austria, and 189 from Switzerland. The analysis focuses on and combines all German speaking respondents and treats them as one answering pool. American statistics are reported on separately in order to be able to compare potential differences that may be due to cultural differences (Hofstede, 1984); 567 questionnaires were not included in the analysis due to the widely distributed national heritages and small samples per nationality.

The number of questionnaires filled in suggests that around 25% of those who have come in touch with the software participated in the survey. This participation rate is high given that privacy

Related Content

Trust Management and Context-Driven Access Control

Paolo Bellavista, Rebecca Montanari, Daniela Tibaldiand Alessandra Toninelli (2008). *Handbook of Research on Wireless Security (pp. 461-478).*

www.irma-international.org/chapter/trust-management-context-driven-access/22064

Towards Usable Application-Oriented Access Controls: Qualitative Results from a Usability Study of SELinux, AppArmor and FBAC-LSM

Z. Cliffe Schreuders, Tanya McGilland Christian Payne (2012). *International Journal of Information Security and Privacy (pp. 57-76).*

www.irma-international.org/article/towards-usable-application-oriented-access/64346

Data Mining Used for Analyzing the Bankruptcy Risk of the Romanian SMEs

Laura Giurca Vasilescu, Marian Siminica, Cerasela Pirvu, Costel Ionascuand Anca Mehedintu (2011). *Surveillance Technologies and Early Warning Systems: Data Mining Applications for Risk Detection (pp. 144-171).*

www.irma-international.org/chapter/data-mining-used-analyzing-bankruptcy/46809

Supply Chain Disruptions and Best-Practice Mitigation Strategies

Adenike Aderonke Moradeyo (2012). *International Journal of Risk and Contingency Management (pp. 45-58).*

www.irma-international.org/article/supply-chain-disruptions-best-practice/70232

Cyber Terrorism and the Contemporary Corporation

Matthew Warrenand William Hutchinson (2001). *Information Security Management: Global Challenges in the New Millennium (pp. 53-64).*

www.irma-international.org/chapter/cyber-terrorism-contemporary-corporation/23360