Chapter XXXVIII
Spyware

Mathias Klang
University of Lund, Sweden & University of Göteborg, Sweden

ABSTRACT

It is well known that technology can be use as to effectively monitor the behavior of crows and individuals and in many cases this knowledge may b the motivation for people to behave differently than if they were not under surveillance. This internalization of surveillance has been widely discussed in privacy literature. Recent software developments have created new threats to the integrity of the individual. Today a form of software, commonly known as spyware, poses an increased threat of covert surveillance. Computer users subjected to spyware are often unaware of the surveillance and therefore continue to behave in a natural manner. This chapter argues that the integrity of the computer user is not protected under law and any rights the user may believe she has are easily circumvented.

INTRODUCTION

This chapter discusses an unusual type of surveillance software, which may be installed in many computers. The strange aspect of this software is that it has often been downloaded and installed by the user, but without her knowledge. The software is mainly designed to collect information about the user of the computer and relay this information back to the software manufacturer. The download, installation, data collection and data transfer all take place within the users own computer but very seldom with the users knowledge (Freeman & Urbaczewski 2005, Zhang 2005). This chapter deals with the issue of a class of monitoring software that gathers information about the computer user and sends the information to another entity the users consent or knowledge commonly referred to as Spyware (Stafford & Urbaczewski 2004, Urbach & Kibel 2004).

It is the intention of this chapter to describe the technology involved and thereafter discuss how this new technology is affecting the online privacy debate. The chapter continues to discuss the basis for legitimacy of technology and also the current level of technological deterrents available. The chapter concludes with a comparison of two approaches at resolving the current problem, via legislation or the market approach.

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

Integrity is a prerequisite for democracy. The perceived lack of integrity causes concern among users. This concern was however met with a regulatory inertia since the apparent legal position of the software in question could be disputed. This lack of concern for the users opinions vis-à-vis integrity resulted in the creation of a market based regulatory solutions. These solutions came in the form of integrity protecting, Spyware removal software.

The earliest uses of the term Spyware to denote a particular form of software that gathers, without the users knowledge, information about the user and transmits it back manufacturer appeared around 2000 (Zone Alarm 2000).

The importance of the discussion of Spyware lies in the discussion of control of user data and user control over the personal computer. Despite being installed via deceit (Klang 2004) those discussing the effects of Spyware on user integrity and privacy issues were aware of the fact that causing Spyware to be installed was not an illegal act. Therefore the discussion becomes a practical definition and implementation of the concept of online privacy. Groups of actors perceived Spyware to be a threat to individual privacy despite the uncertain legal position gives Spyware manufacturers an upper hand.

The failing ability of regulatory structures to provide protection against the perceived threat of Spyware create the rise of a market based solution where software manufacturers created anti-Spyware software to provide users the wherewithal to prevent Spyware from operating within their computers. The example of Spyware provides an excellent case of the failure of structural regulation, the rise of a perceived threat among actors and the development of a market-based solution to the perceived threat. By studying this example we may find a method where the slowness of structural regulation to react to a perceived user threat provides both an economic opportunity for actors and provides an example of how online problems can be resolved without the intervention of regulatory structures.

PRIVACY

The discussion of privacy as a philosophical, social and legal value has been lively ever since the publication in 1890 of the influential paper, *The Right to Privacy* (Warren & Brandeis 1890). Arguably the clearest conclusion from this long debate is that the interpretation of privacy is context dependent. However despite the width of the arguments most can be categorised either as belonging to the reductionist approach or by viewing privacy a necessary individual right (Thompson 1975). The reductionist approach understands privacy as being described by its component parts while ignoring the relationships between them. This is the view that privacy is not unique and can be reduced to other interests. The second approach to privacy is to see it as a fundamental human need or right and therefore it needs not be derived from other rights. Thompson (1975) argues that privacy is not an individual right but can be motivated and defended by using other rights, which makes the right to privacy *per se* unnecessary:

For if I am right, the right to privacy is 'derivative' in this sense: it is possible to explain in the case of each right in the cluster how come we have it without even once mentioning the right to privacy. Indeed, the wrongness of every violation of the right to privacy can be explained without even once mentioning it. (Thompson, p. 313).

Posner (1984) argues for the reductionist approach by using an economic analysis of privacy. He argues that "personal privacy seems to be valued more highly than organizational privacy, a reverse ordering would be more consistent with the economics of the problem." The reductionist arguments have often been attacked by scholars

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/spyware/21605

Related Content

Robots and the Ethics of Care
Linda Johansson (2013). *International Journal of Technoethics (pp. 67-82).*
www.irma-international.org/article/robots-ethics-care/77368

Two Spatial Watermarking Techniques for Digital Images
Dumitru Dan Burdescu, Liana Stanescuand Marian Cristian Mihaescu (2013). *Digital Rights Management: Concepts, Methodologies, Tools, and Applications (pp. 691-712).*
www.irma-international.org/chapter/two-spatial-watermarking-techniques-digital/70997

The Porn Drift: Pornography, Technology and Masturbation
Mitja Suni (2013). *International Journal of Technoethics (pp. 58-71).*
www.irma-international.org/article/the-porn-drift/90489

Online and Offline Content Piracy Activities: Characteristics and Ethical Perceptions
Troy J. Strader, J. Royce Fichtner, Geoffrey D. Bartlettand Lou Ann Simpson (2014). *International Journal of Technoethics (pp. 22-36).*
www.irma-international.org/article/online-and-offline-content-piracy-activities/116718

“Revenge Porn”: An Analysis of Legislative and Policy Responses
Terry Goldsworthy, Matthew Rajand Joseph Crowley (2017). *International Journal of Technoethics (pp. 26-41).*
www.irma-international.org/article/revenge-porn/181648