Cyber Citizens and Cyber Deviance: Exploring Social and Technical Factors as Antecedents to Cyber Deviance and the Implications for Cyber Citizenship

Richelle L. Oakley  
*University of North Carolina at Greensboro, rloakle3@uncg.edu*

A. F. Salam  
*University of North Carolina at Greensboro, a_f_salam@uncg.edu*

Follow this and additional works at: [http://aisel.aisnet.org/sighci2012](http://aisel.aisnet.org/sighci2012)

**Recommended Citation**
[http://aisel.aisnet.org/sighci2012/7](http://aisel.aisnet.org/sighci2012/7)
Cyber Citizens and Cyber Deviance: Exploring Social and Technical Factors as Antecedents to Cyber Deviance and the Implications for Cyber Citizenship

Richelle L. Oakley  
ISSCM Department  
Bryan School of Business and Economics  
The University of North Carolina at Greensboro  
Greensboro, NC 27402 USA  
rloakle3@uncg.edu

A. F. Salam  
ISSCM Department  
Bryan School of Business and Economics  
The University of North Carolina at Greensboro  
Greensboro, NC 27402 USA  
A_F_Salam@uncg.edu

ABSTRACT

There is an alarming trend of individuals behaving inappropriately with information technology in both organizational and personal settings. For example, in a work context individuals are breaking repeatedly security protocols (Hovav et al. 2011) leading to the compromise of sensitive customer and important organizational data resources. Information systems (IS) researchers have studied the manners by which employees use, and misuse, information technology within organizations (Warkentin et al. 2009). Alternatively, in a non-work context, attention has been given to digital media piracy (Siponen et al. 2012) which continues to plague organizations. These examples illustrate some unacceptable behaviors exhibited by cyber citizens (Anderson et al. 2010) – both in the work and non-work settings.

Typically, the boundaries of acceptable and unacceptable cyber behavior are defined by government authorities, who develop laws around specific illegal online behaviors, and businesses, who detail inappropriate actions in their terms of service agreements. Past research has shown that even with detailed guidelines, employees continue to cause breaches in security (Harris 2012) and these actions are greatly influenced by the behaviors of their coworkers (Gallivan et al. 2005).

Alternatively, in a non-work environment, computer users operate within a precarious social and technological environment where the guidelines on appropriate behavior are vague (Nowak 2011). In such an ill-defined context, individuals tend to refer to accepted social norms as a guide, rather than try to understand the disparity between laws and policies (Morrison 1994).

Research in criminology, sociology, and management, has focused on deviant behaviors with technology, termed cyber deviance. This term refers to inappropriate or criminal behavior in a digital context (Holt et al. 2010). Technical solutions are only marginally effective as deviant cyber behavior continues to proliferate (Rogers et al. 2006). Research has examined individual factors, such as self-control, in order to explain cyber deviant behaviors (Hinduja et al. 2008). Social factors have begun to be examined through the use of social learning theory and social cognitive theory to explain the ways in which attitudes and beliefs influence cyber deviance (Jacobs et al. 2012). Although studies that examine the individual, social, and technical factors have provided insight into cyber deviance behavior, they have not considered such behavior as part of cyber citizenship, where individuals behave in an ethical and productive manner in online environments. Additionally, recent IS research has begun to explore alternative ways to influence social norms and attitudes on individual behaviors in online environments in order to create more conscientious cyber citizens (Anderson et al. 2010).

Therefore, this study aims to examine the individual, social, and technical factors that impact one’s intention to engage in cyber deviance. In this study, we focus on the illegal activities that occur in a digital environment. This highlights the unique actions that occur between humans and technology, suggesting this study is best served from such a perspective. Scialdone (2010) provides human computer interaction (HCI) researchers with a useful framework for examining phenomena that occur between humans and technology. Researchers must identify the human, the technology, the tasks, and the context to clearly situate their study in the HCI literature (Scialdone 2010).

In this study we focus on average PC users and their interactions in computer-mediated social networks (CMSN). We examine individual factors, Perceived Utility of Cyber Deviance and Self-efficacy in Cyber Deviance; social factors, Cyber Citizen Social Norms on Cyber Deviance, and technical factors, CMSN Influencer and CMSN Intensity. The proposed research methodology is a quantitative approach using a quasi-experimental setup (Bhattacherjee 2012) through the use of scenarios which describe situations of cyber deviance. The use of scenarios allows us to provide a specific situation which serves as a reference point for our inquiry into the concepts of interest (Nagin and Paternoster 1993).