The Dark Internet: Without Darkness There is No Light

Panel

Joey F. George
Iowa State University
jfgeorge@iastate.edu

Douglas Derrick
University of Nebraska at Omaha
dcderrick@unomaha.edu

Andrew Harrison
University of Cincinnati
harri3ar@ucmail.uc.edu

Kent Marett
Mississippi State University
kmarett@business.msstate.edu

Jason B. Thatcher
Clemson University
jthatch@clemson.edu

ABSTRACT

What is the Bright Internet? One way to define ‘bright’ is to explore darkness. The purpose of this panel is to clarify what is meant by the ‘Bright Internet’ by presenting the contrast of the ‘Dark Internet’ and the dark web. The panelists, all of whom have expertise in the dark side of Internet and information technology use, will discuss deception, fraud, phishing, terrorism, and the dark web.

Keywords

Internet, bright internet, dark web, deception, fraud, phishing, terrorism

PANEL OVERVIEW AND OBJECTIVE

“They say there is no light without dark, no good without evil, no male without female, no right without wrong. That nothing can exist if it's direct opposite does not also exist.”

― Laurell K. Hamilton, *Incubus Dreams*

The governing Council of the Association for Information Systems (AIS) has adopted an initiative for the promotion of the “Bright Internet.” In the words of AIS President Jae Kyu Lee, the goal of the initiative is to “provide the foundation of the framework for a new and safer Internet platform, the *Bright Internet*, while protecting users’ privacy at an appropriate level (Lee, 2015).” Activities designed to promote the initiative have included panels at various information systems conferences, a guest editorial in *MIS Quarterly*, and the signing of a memorandum of understanding with the United Nations body, the International Telecommunication Union (ITU) in 2015.

Despite these efforts, it is not entirely clear just what is meant by the Bright Internet. In an effort to bring further clarity to this term, we here explore what might be called the “Dark Internet” (not the same as the dark web). Without darkness, there can be no light, so recognizing and defining the darkness should make the light (or bright) more clear.

The idea of a dark side of information technology use is not new (George, 1996). Kim and colleagues developed a taxonomy of the dark side of the Internet (Kim, Jeong, Kim & So, 2011), which provides lists of problematic activities from both a technology and non-technology perspective (Table 1). Recent attempts at bringing attention to the dark side include two special issues of *Information Systems Journal* (Tarafdar, Gupta & Turel, 2015a & 2015b). Among the topics of the dark side oriented papers in the special issues were: The illegal sharing of music files, computer abuse, technostress, IT interruptions and their effect on productivity, computer-mediated control, and computer addiction.

Although these abuses of the Internet and these unanticipated consequences of information technology use are serious and have real implications, it might actually be more accurate to portray them as a lighter shade of dark, given the truly dark and harmful aspects of what is called the dark web (Gehl, 2014). The dark web, accessible only through the Onion Router (Tor), provides a platform to support such activities as child pornography, the drug market (e.g. Silk Road), the gun trade, killers for hire, and terrorists. However, since Edward Snowden’s revelations about the National Security Agency’s surveillance activities, Tor usage has increased for those who want to communicate more freely and anonymously, such as Chinese dissidents and victims of domestic abuse, none of whom want to be tracked (Gehl, 2014)

Technology -centric	Spam
	Malware
	Hacking
	Denial of service attacks
	Phishing
	Click fraud
	Violation of digital property rights
Non-technology-centric	Online theft
	Online scams and frauds
	Cyber bullying
	Spreading of false or private information
	Illegal online gambling
	Aiding crime
	Other reprehensible behaviors

Table 1: Taxonomy of the dark side of the Internet, from Kim et al 2011

The purpose of this panel is to explore the dark side of the Internet, both the dark and the truly dark, with the intention of more clearly defining the “Bright Internet” by focusing on what it is not. Our hope is that a meditation on the potential for darkness will clarify the light and reinforce the idea that one cannot exist without the other. To that end, we discuss three topics from the routinely dark side, deception, fraud and phishing, and two topics from the truly dark side, terrorism and the dark web. We end the panel with some comments on the implications for AIS’s Bright Internet initiative.

PANEL LAYOUT

The panel will begin with an introduction of the topic and the panel by the moderator. Each panelist, including the moderator will take 10 minutes to lay out their particular expertise in the dark Internet. The presentations will progress from mildly dark to truly dark: computer-mediated deceptive communication (Joey George); fraud (Andrew Harrison); phishing (Kent Marett); terrorism (Douglas Derrick); the dark web (Jason Thatcher). The audience will then be invited to join in with questions and comments. With 10 minutes left, each panelist will make a brief statement about the implications of the dark Internet for the AIS Bright Internet initiative and human behavior related to information technology generally.

PANEL PARTICIPANTS

Joey F. George is Professor of Information Systems and the DeVries Endowed Chair in Business in the College of Business at Iowa State University. He has studied deception for over 20 years. He was the Editor-in-Chief of *Communications of the Association for Information Systems* and Senior Editor for *MIS Quarterly* and *Information Systems Research*. He is a past President of the Association for Information Systems, an AIS Fellow, and recipient of the AIS LEO award. He will moderate the panel and discuss deceptive computer-mediated communication and its dark implications.

Douglas Derrick is an Assistant Professor in the School of Interdisciplinary Informatics in the Peter Kiewit Institute at the University of Nebraska at Omaha. He earned his Ph.D. in MIS from the University of Arizona. His research has focused on deception and intent detection, including the development of an automated immigration control system. During the panel, he will discuss his recent research on ISIL and its use of social media and the Internet for recruiting and propaganda purposes.

Andrew Harrison is an Assistant Professor of Information Systems in the Lindner School of Business at the University of Cincinnati. His research focuses on how technologies influence online fraud behaviors. His research studies investigate dark internet topics including: how media capabilities affect fraud rationalization, employees’ willingness to misuse customer data, and the impact of the dark triad of personality characteristics (i.e., narcissism, Machiavellianism, and psychopathy) on fraud. During the panel, he will speak about the growth of online consumer fraud and the challenges associated with its deterrence, detection, and punishment.

Kent Marett is an Associate Professor of Business Information Systems at Mississippi State University. He has helped coordinate research projects on phishing, social engineering, and online deceptive techniques, leading to articles published in journals such as *Information Systems Research*, the *Journal of Management Information Systems*, and *Group Decision & Negotiation*. He is also currently working on improving the “soft skills” security practices for employees and managers in rural small-to-medium sized businesses. He will address the topic of phishing during the panel. Phishing has been around for years, but methods have gotten more sophisticated with time (as with "spear phishing"). Kent will explore current trends in phishing and what researchers and organizations are currently planning to help cast light on this old problem.

Jason Thatcher is a President-Elect of the Association for Information Systems and Professor in the Department of Management at Clemson University. Dr. Thatcher's research examines the influence of individual beliefs and characteristics on adaptive and maladaptive post-adoption information technology use. His work has resulted in the development of IT artifacts, been funded by the National Science Foundation, SalesForce.com, and IBM, and appeared in refereed journal outlets such as *MISQ Quarterly* and *Information Systems Research*. He will discuss challenges connected to conducting funded research on the Dark Web. Specifically, he will discuss projects designed to develop tools to enable scholarly enquiry using real-time and archival data drawn from heterogeneous data drawn from the Dark Web, online social networks, and other sources.

EQUIPMENT REQUIREMENTS

We have no special equipment requirements.

REFERENCES

1. Gehl, R.W. (2014). Power/freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network, *new media & society*, accessed at nms.sagepub.com, 2/27/16.
2. George, J.F. (1996). Computer-Based Monitoring: Common Perceptions and Empirical Results, *MIS Quarterly*, 20, 4, 459-480
3. Kim, W., Jeong, O-R, Kim, C., & So, J. (2011). The Dark Side of the Internet: Attacks, Costs and Responses, *Information Systems*, 36, 675-705.
4. Lee, J.K. (2015). Guest Editorial: Research Framework for AIS Grand Vision of the Bright ICT Initiative, *MIS Quarterly*, 39, 2, iii-xii.
5. Tarafdar, M., Gupta, A., & Turel, O. (2015a). Special Issue on 'Dark Side of Information Technology Use': An Introduction and a Framework for Research, *Information Systems Journal*, 25, 161-170.
6. Tarafdar, M., Gupta, A., & Turel, O. (2015b). Introduction to the Special Issue on 'Dark Side of Information Technology Use' – Part Two, *Information Systems Journal*, 25, 315-317.