Pacific Asia Journal of the Association for Information Systems

Volume 3 | Issue 4 Article 2

12-1-2011

Privacy and Security Aspects of Social Media: Institutional and Technological Environment

Nir Kshetri
University of North Carolina, nbkshetr@uncg.edu

Privacy and Security Aspects of Social Media: Institutional and Technological Environment

Nir Kshetri
Bryan School of Business and Economics
The University of North Carolina at Greensboro
nbkshetr@uncg.edu

Abstract

Legitimate as well as illegitimate organizations and entities are gaining access to information about social media (SM) users through illegal, extralegal, and quasi-legal means. Worse still, many organizations and individuals using SM have become targets and victims of cybercrimes. SM have also led to an exposure of unethical and illegal conducts within some organizations. One estimate suggested that 36% of social networking users have reported experiencing malware attacks through their profiles. Another study suggested that one in four companies have become cybercrime victims via social networking sites. Likewise, about a quarter of employers surveyed by the Society of Corporate Compliance and Ethics in 2009 had disciplined an employee for improper activities on social networking sites. Organizations that fail to take appropriate technological and behavioral measures related to SM are likely to suffer reputation damages, loss of customers' confidence, and other types of economic losses. The goal of this paper is to develop a framework that provides a simple, explicit mechanism for understanding privacy and security issues associated with SM. To achieve this goal, we draw upon literatures on diverse areas such as institutional theory, marketing and criminology. Specifically, we examine how various institutions from the standpoint of SM superimpose in a unique interaction with SM related technologies' natures that influence businesses' and consumers' privacy and security. We discuss how various features of SM related technologies such as newness (leading to ineffectiveness of existing IT security products), complexity (difficulty to understand SM's functioning) and attractiveness of SM as a cybercrime target (availability of information with superior targetability and huge size and rapid growth of SM). We also examine how regulative institutions (lack of laws to deal with SM as well as lack of enforcement of existing laws), normative institutions (lack of ethical and professional guidelines) and cognitive institutions (lack of precautionary measures and lack of defensive measures or counterpoison) have contributed to a lack of behavioral and attitudinal measures to ensure privacy and security.

Keywords: Social Media, Rare Enemy Syndrome, Targetability, Privacy and Security, Institutions

Introduction

The rapid growth of social media (SM) has posed fundamental security and privacy challenges. SM have attracted various actors that engage in illegal, extra-legal, and sometimes criminal activities. As evidenced by the recent attacks on Twitter, Facebook, and MySpace, cyber-criminals are exploiting the viral nature of Web 2.0 and social networking sites (Kshetri, 2010a). In April 2010, the U.K.'s Nottinghamshire Police reported that crimes associated with Facebook that were reported to the agency (e.g., sex crimes, verbal abuse, assault) increased by 346% during the previous 22 months (Peppiatt, 2010). According to Kaspersky Lab, in the first quarter of 2010, Facebook was the No. 4 most targeted site by phishers, after PayPal, eBay and HSBC (Richmond, 2010).

Preliminary studies indicate a high rate of returns associated with organizations' implementation of SM for marketing activities. A study conducted by vitrue (http://vitrue.com/) indicated that in the average the value of a 'Fan' on SM is $3.60 (Morrissey, 2010). Yet privacy and security concerns have hindered organizations' adoption of SM. For instance, companies are increasingly limiting their employees' access to social networking sites. Yet, about a quarter of employers surveyed by the Society of Corporate Compliance and Ethics in 2009 had disciplined at least one employee for improper activities on social networking sites (Chen, 2010). A survey commissioned by Robert Half Technology found that 21 % of chief information officers have limited the personal use of SM sites in the workplace. Note that a previous survey commissioned by Robert Half Technology found that 58 % of companies have banned SM sites altogether (Magder, 2010). A study by Sophos indicates that 12-17% of organizations surveyed control access to social networking sites due to concerns related to malware and data leakage (Lardinois, 2009).

Experts argue that in order to prevent cybercrimes, it is important for users and platform owners to consider the ethical, legal, and technical issues associated with SM (Chretien, Ryan, Chretien and Kind, 2009; Lagu, Kaufman, Asch, and Armstrong, 2010; Ramsey and Venkatesan, 2010; Thompson, Dawson and Ferdig, 2008). The productive use of SM in marketing activities, tempered with an appropriate level of privacy and security, is a strategic policy action item, and, a theoretical issue that adjoins broad-based substantive interests within marketing to various social science disciplines. Although prior researchers have acknowledged the role of SM, they have paid relatively less attention to how privacy and security issues are affecting the diffusion patterns of SM. Thus, it is important for managers to better understand privacy and security issues associated with SM.

The purpose of our study is to contribute to filling this void. We examine how institutional and technological environments are linked to behavioral and attitudinal measures to ensure privacy and security in SM. We develop a framework that provides a simple, explicit mechanism for understanding privacy and security issues associated with SM. To achieve this goal, we draw upon literatures on diverse areas such as institutional theory, marketing, and criminology.

The paper is structured as follows. We proceed by first providing a brief survey of privacy and security concerns associated with SM. Next, we examine the institutional and technological environments and relevant issues facing SM. Then, we discuss privacy and security issues within the context of the specific environments and provide some practical implications. The final section provides concluding comments.

Privacy and Security Concerns Associated with SM: A Survey

The rise in privacy and security breaches in SM can be treated as part of a larger trend of the rapid growth in the global cybercrime industry (Kshetri, 2010a). Due to the government's constant public announcements of internet security breaches and pending cyberterrorism, there is a heightened sense of fear and anxiety about cybercrimes involving SM among individuals and businesses. In this

section, we organize the discussion by focusing separately on privacy and security issues facing businesses and consumers and also on various forms of cybercrimes associated with SM, which can be considered as a conceptual superset of privacy and security issues.

Impacts on businesses

A survey conducted by IBM found that U.S. businesses worry more about cybercrimes than about physical crimes (Christian Science Monitor, 2006). One estimate suggested that one in four companies report attacks via social networking sites (Kaplan, 2009). Advertisers have been complaining about click fraud of up to 100% (Techcrunch.com, 2009). Note that a large proportion of Facebook revenue comes from pay-per-click (PPC) advertising from small self-serve advertisers. It is reported that some advertisers spend $30,000 a day on ads on Facebook (Arrington, 2009). SM are also associated with threats such as phishing and the leakage of intellectual property (Kavur, 2010). According to a study by Open DNS (www.opendns.com) Facebook was the second biggest phishing target after PayPal and was the most blocked website by companies (Cooter, 2011).

Impacts on consumers

An IBM survey released in 2006 found that there were three times more Americans, who thought they would be more likely victims of a computer crime "in the next year" than of a physical crime (Keizer, 2006). According to Consumer Reports' State of the Net survey released in May 2010, 9% of social network users experienced some forms of abuse within the past year (e.g., malware infections, scams, identity theft or harassment) (Woollacott, 2010). In June 2009, laptops of several business school students at Yale University were simultaneously infected, which was suspected to have spread through Facebook (Finkle, 2009). Cyber-criminals have also targeted Twitter users by using links with malware that tag current topics (Voigt, 2009).

Cyber-criminals' actions are centered around popular SM activities. One of them, for instance, is online games. A Cisco study released in July 2010 indicated that 7% of Facebook users across the world access the site to play the interactive game, Farmville, which its users spend an average of 68 minutes a day on virtual farming. Likewise, another game, Mafia Wars, is played by 5% of Facebook users daily. Each user that played Mafia Wars spent 52 minutes on the game while at work. Cisco believes that cyber-criminals are developing ways to deliver malware via these games (The Straits Times, 2010).

Types and classification of cybercrimes associated with SM

Glaser (1971) identified and classified various types of crimes, including: predatory crimes against property, predatory crimes against person, illegal service crimes, and public disorder crimes. Most of these can be extended in the context of the cyberspace, more specifically into SM. Cyber attacks can be classified using various criteria. One way to classify them is to consider whether they are directed against an intended target (e.g., targeted and opportunistic attacks) or are just broad-stroke targeting. Cyber attacks can also be classified into two categories based on whether they are predatory or market-based. A further way to classify cybercrimes is related to the relative roles of human and technology elements-- Type I and Type II cybercrimes.

Targeted vs. opportunistic attacks

In targeted attacks, specific tools are used against specific SM targets. Targeted attacks are carried out by skilled hackers with expertise to do serious damages. Some of them are motivated by financial gains. Targeted attacks are also initiated by terrorists, rival companies (e.g., click frauds in Facebook), ideological hackers and/or government agencies. Hackers that were initially involved in mass attacks are moving towards more sophisticated focused attacks that target SM sites.

Opportunistic attacks, on the other hand, entail releasing worms and viruses that spread indiscriminately across the Internet. Oppor-

tunistic attacks are less dangerous than targeted attacks and have smaller financial ramifications.

Predatory cybercrimes vs. market-based cybercrimes

Cybercrimes can also be grouped into two types: predatory cybercrimes for profit and market-based cybercrimes (Naylor, 2005). Predatory cybercrimes can be defined as illegal acts in the cyberspace in which "someone definitely and intentionally takes or damages the person or property of another" (Glaser, 1971). An example could be stealing money from someone's bank account using the information fraudulently received from SM users. From the national GNP point of view, these acts do not produce new goods or services. They simply redistribute the existing wealth. Market-based cybercrimes, on the other hand, generate new incomes rather than redistributing the existing wealth (Naylor, 2005). Such crimes occur, for example, in the sales of stolen credit card information and illegal drugs online.

Type I and Type II cybercrimes involving SM

Gordon and Ford (2006) have divided cybercrime into distinct categories. In their categorization, Type I cybercrime mostly contains technological elements, such as malware attacks via social-networking sites, which are growing in volume recently (Whitney, 2010). A study estimated that 36% of social networking users reported experiencing malware attacks through their profiles (Tuazon and Mark, 2010). It should be noted that login details from social networking websites can also be bought in the underground economy. The Sydney Morning Herald (2010) reported that a Russian hacker known as "Kirllos," who was living in New Zealand, was offering the login details (i.e. usernames and passwords) of 1.5 million Facebook users. The price was NZ$62.70 (about US$ 44) per 1000 accounts sold on an underground hacker forum.

Type II cybercrimes have mainly human elements (Gordon and Ford, 2006). Turning now to the specific context of cybercrimes targeting SM sites, it is important to note that crimes such as "Facebook phishing" are rising. It is possible that a cyber-criminal may claim to be a friend and convince a Facebook user to share his/her password. This is a very serious security breach since over 50% Facebook users were found to employ the same password for their individual bank accounts (Rodgers, 2009).

Institutional and Technological Environment Facing SM

As a visual aid, Figure 1 schematically represents how privacy and security issues in SM, and more broadly cybercrimes, are tightly linked to the institutional and technological environment. We discuss building blocks of the model in this section. An understanding of model would help organizations take technological, behavioral and perceptual/attitudinal measures to combat the threat of cybercrime. Organizations that fail to take appropriate technological and behavioral measures related to SM are likely to suffer reputation damages, loss of customers' confidence, and other types of economic losses (Figure 1).

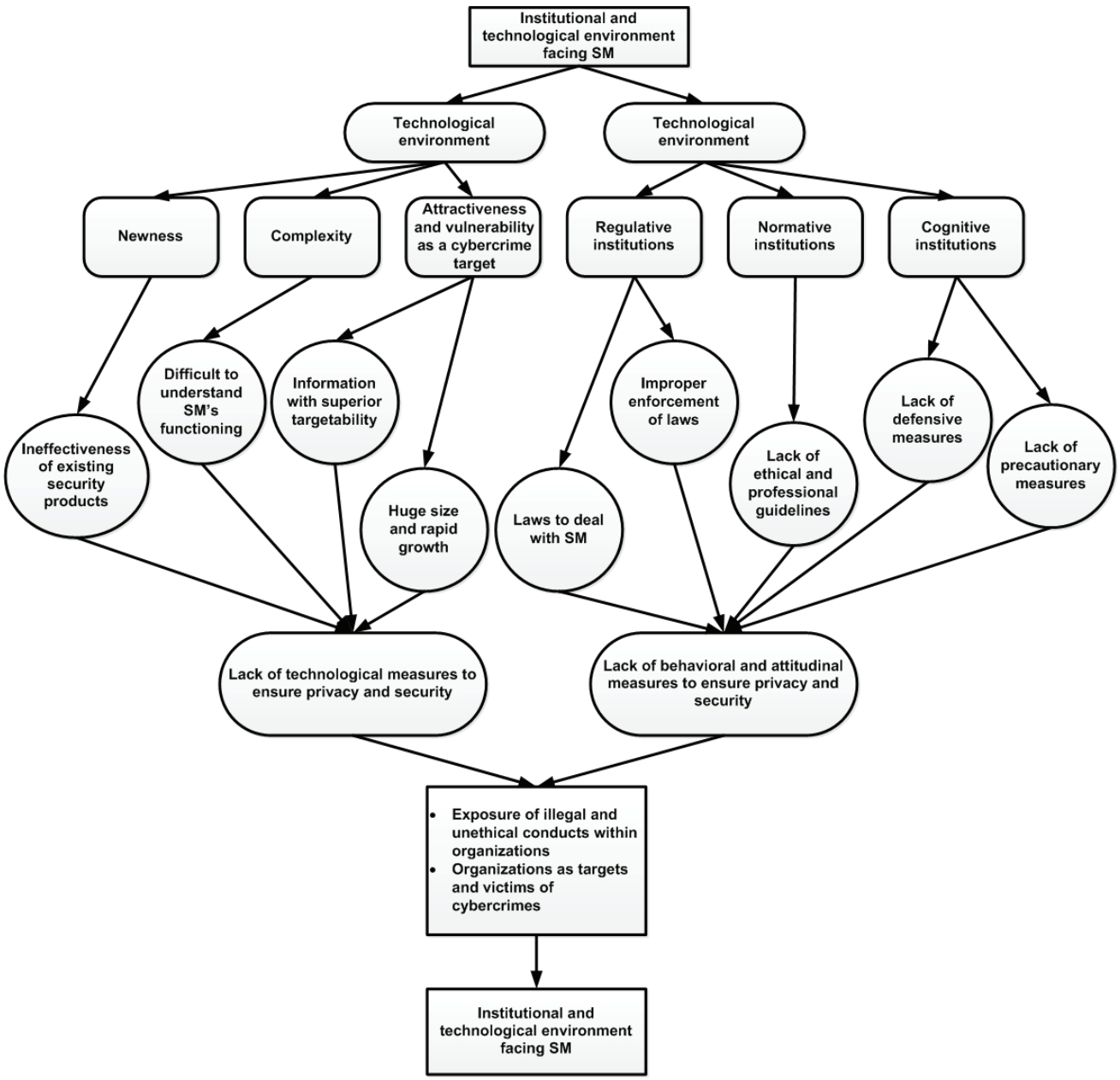
Technological Environment

A firm's strategy is tightly linked to the technological environment within which it is operating (Audretsch, 1991). In this paper's context, we discuss three main characteristics of technologies enabling SM: newness, complexity, and superior targetability. Let's take a look at each of the components in turn.

Newness

The number of malware products targeting social networking sites is increasing rapidly. One estimate suggested that the number of malware products spreading via social networking sites increased from about 10,000 in 2007 to over 25,000 during 2008 (Tanase, 2010). Cyber-criminals are attracted by SM sites' economies of scale and effectiveness. Due to the newness of SM, however, most existing IT security products are ineffective. Many SM sites are found to contain vulnerabilities that are undetectable and untraceable to most available security technologies.

Figure 1 - A framework for understanding security and privacy issues facing SM



For instance, IT security products (such as, Web filtering, firewalls and network security devices) are inadequate to deal with malware targeting SM sites (Kavur, 2010). In sum, conventional security software is of little help to deal with vulnerabilities involving SM (Null, 2001).

Complexity

Another problem concerns the difficulty in understanding SM's functioning. Experts have, for instance, complained that SM users are not given simple ways to understand "what personal information is being made available to whom" (Marks, 2010). Cowan (2010) has

summarized complexity in Facebook's privacy measures best: "Rapid growth, a pile-up of new features and ad hoc responses to previous privacy concerns meant the site's privacy controls had become maddeningly complex, with users required to navigate 50 different settings and 170 different options".

We can further illustrate SM's complexity with an example of Facebook ads. Before we proceed, it is important to note that Facebook served 176.3 billion ads in the first quarter of 2010, which is more than by Yahoo (Cowan, 2010). Note that ads work differently in Facebook compared to search engines such as Google and yahoo. While an ad can be seen on the parked domain page, or when an Internet users types in a keyword, it may not be possible to see a Facebook ad. This is because Facebook ads are "hyper targeted" based on "deep demographic data" (Tanase, 2010). For instance, using the self-serve ads, an advertiser can target "users that are female, aged 13-17, and, who live in San Francisco" (Cutler and Marshal, 2009). A user that does not fit this profile does not see the ad.

Facebook advertisers have claimed that their ads are clicked by competitors, leading to higher costs (Arrington, 2009). A high level of complexity may make it difficult for an advertiser to track fraudulent activities associated with an ad.

The rise of cybercrimes targeting social network users is also associated with and facilitated by the proliferation of third party applications on various SM platforms (Ramsey and Venkatesan, 2010). For one thing, they have increased complexity. Many such applications allow users to store, organize and exchange information. In April 2010, Facebook started giving third-party applications more access to user data (Fletcher and Ford, 2010). Some Apps, which used to be allowed to keep user data only for 24 hours, can store them indefinitely unless users uninstall them. Facebook Instant Personalization launched in spring 2010 lets businesses create recommendation based on user data (Fletcher and Ford, 2010).

Most impressive, as of July 2010, the independent developer, Zynga was estimated to have 235 million active Facebook users a month playing games developed by the company (foreign.peacefmonline.com, 2010). A common complaint about many applications developed by independent programmers, however, is that there has been a lack of basic security measures and procedures in these apps (Soghoian, 2008). Worse still, some are designed to steal personal information. A case in point is the Facebook application, "Dislike" button recently created by a third-party developer. This was reported to be a malware, which created revenue for its developer when users completed a survey. It also gave the developer access to personal data and used Facebook accounts for generating spam messages (Pert, 2010). In August 2010, Facebook Security (http://www.facebook.com/security) issued a warning about the bogus Dislike button scam.

Targetability

In the context of this paper, targetability is related to a legitimate or illegitimate organization's capability to reach an attractive target.

Attractiveness of SM as a cybercrime target

Two explanations related to attractiveness of SM can be suggested for the rapid growth of cybercrimes targeting SM. A simple, straightforward explanation is that cyber-criminals consider SM sites as a lucrative target due to their rapid growth. One estimate suggested that, as of July 2010, 74% of the world's Internet population visited social networking sites, and in the average, Internet users spent an average of six hours per month on such sites (nielsen.com, 2010). The number of people using Facebook reached 500 million on 21 July 2010 (Pepitone, 2010). Particularly, South Korea's leading social media site, Naver, was reported to attract 95% of the country's Internet population every month (nielsen.com, 2010). Likewise, eight out of the top 20 websites in the UAE incorporate SM elements (McArthur, 2010).

A second factor related to attractiveness (and often associated with privacy violation and

security breaches on SM sites) is data quality. Data and information that is available on such sites are of superior quality. Unsurprisingly, legitimate enterprises, as well, as criminal outfits find it too tempting to self-regulate, and often actively seek to covertly gain access to the best quality information available in SM networks. It is important to note that target attractiveness depends on offenders' perceptions of victims (Kshetri, 2010a). A lawsuit filed in August 2009 five individuals in the Orange County Superior Court claimed that Facebook's business model is "designed to harvest as much personal and private information as possible in easiest, quickest, and most innocuous-looking manner possible", which is shared with "third parties for commercial purposes and economic benefit" (softpedia.com, 2009).

Prior research indicates that crime opportunity is a function of target attractiveness, which is measured in monetary or symbolic value and portability (Clarke, 1995). In this regard, availability of information with superior targetability, as well as, huge size and rapid growth make SM as an attractive target for cyber-criminals. In summary, SM's popularity, as well, as the amount and quality of information stored on SM platforms make them an attractive cybercrime target (Ramsey and Venkatesan, 2010).

Institutional Environment

Institutions are defined as "macro-level rules of the game" (North, 1990, p. 27), which consist of "formal constraints (rules, laws, constitutions), informal constraints (norms of behavior, conventions, and self-imposed codes of conduct), and their enforcement characteristics" (North, 1996). Institutional theory is described as "a theory of legitimacy seeking" (Dickson, BeShers and Gupta, 2004). To gain legitimacy, organizations adopt behaviors irrespective of the effect on organizational efficiency (Campbell, 2004). For instance, it was reported that in China, Microsoft blocks bloggers from posting politically objectionable words and, when Google was operating in the country, it shut down when users looked for sensitive words.

Institutional influence on the SM industry becomes an admittedly complex process (Dickson, BeShers and Gupta, 2004) when organizations have to derive legitimacy from multiple sources such as employees, clients, local communities, professional and trade associations and governments. Scott (2001) proposed three institutional pillars: (i) regulative; (ii) normative and (iii) cognitive. These pillars relate to "legally sanctioned", "morally governed" and "recognizable, taken-for-granted" behaviors respectively (Scott, Ruef, Mendel, and Caronna, 2000).

An important point to note is that institutional actors' responses lag behind the technological changes (Brenner, 2004; Katyal, 2001; Kshetri, 2010a). This can be attributed to institutional inertia. Moreover, institutional actors vary in their timing of responses to a given change in technology.

Regulative Institutions

Lack of laws to deal with SM

The SM industry legal system is evolving more slowly compared to the SM technology development. As of August 2010, only three countries in the world-- the UK, New Zealand and Australia-- had developed legal framework on the use of SM for litigation purposes (Kowalski, 2010). In August 2010, Singapore's Supreme Court has released a Consultation Paper on the use of SM for litigation purposes including service of documents (Supreme Court of Singapore 2010). Singapore is expected to be the fourth country to have a comprehensive legal framework on SM.

Until 2009, the U.S. did not have a law which held marketers liable for false statements published on blogs and social networking websites. In 2009, the FTC revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising. The revision defined instances in which a blogger's relationship with a company is necessary to disclose to avoid misleading consumers (Sullivan, 2009). This was the FTC's first revision in its guidelines for endorsements and testimonials since 1980 (Kee, 2009).

Moreover, some economies' existing laws have been ineffective to deal with fraudulent activities associated with SM. For instance, consider differences between the approaches of China and the U.S in dealing with astroturfing in SM. Note that astroturfing is political, advertising, or public relations campaigns that are formally planned by an organization, but are designed to mask the nature of the originator in an attempt to create the illusion of being spontaneous, popular, and "grassroots" behavior. SM have opened a new avenue for astroturfers. It was reported that, in New York State, a cosmetic surgery company had its employees pretend to be satisfied customers in writing online testimonials. In 2009, the New York attorney general received a $300,000 settlement from the company for this action (Lazar, 2010).

Similarly, a *Business Week* article (June 23, 2008) reported that China's public relations firms such as Daqi.com, Chinese Web Union and CIC charge US$500-25,000 monthly to monitor online posts. They help minimize the impact of negative information and create positive brand value for the company. There are reports that these PR firms hire students to write good posts about certain brands and to criticize the competition. While critics are concerned about the manipulation of consumer reviews and paid reviews, Astroturfers in China haven't faced legal problems.

One way to understand the China-U.S. difference is to consider their experiences with modern capitalism. Many successful firms in mature market economies are guided by customer orientation and demonstrate their commitment to customer focus. Customers in these economies exhibit a low tolerance for acceptance of poor behavior if businesses and suppliers do not fulfill their implicit and explicit commitments. Due to China's short history of modern capitalism, Chinese clients, and customers are more likely to tolerate an absence of business ethics and a low level of product and service quality and/or reliability.

Improper enforcement of laws

Brenner (2004) notes: ". . . the traditional model of law enforcement is a compilation of past practices that have been deemed effective in dealing with the phenomena it confronts. The model's general strategy, the reactive approach, is one that has been in use since antiquity". Such an approach has been highly ineffective in the SM industry since SM crosses all borders.

In addition to incomplete regulation, criticisms of improper enforcement are also significant. There have been concerns about possible overreach by law enforcement agencies. In the U.S., for instance, thanks to the 2001 Patriot Act, the federal government can ask service providers to submit personal details of an Internet user's online activities without telling the Internet user about it. The FBI's internal audits indicated the possibility of "overreaching" by the agency in accessing Internet users' information (Zittrain, 2009). Unlike the U.S., the Chinese government has no limit on covert monitoring of its citizenry. The Chinese version of Skype instant messaging software is used to monitor texting conversations and will actively block undesirable words and phrases (Zittrain, 2009).

The FBI is reported to be in dilemma regarding the use of fake identities to investigate cybercrimes on SM. According to a FBI document reported by Hoover (2010), despite the potential of undercover operations in gaining access to private information, the agency has expressed concerns that undercover use of personal information may be complicated. If the agents do not use their own name, such information gathering can be considered unauthorized and/or illegal. The agency cited complications over Lori Drew's trial, who was acquitted of cyber-bullying a teen who later committed suicide.

The e-commerce industry is undergoing a major technological upheaval. In such situations, for various actors, the institutional context may not provide organizing templates, models for action, and sources of legitimacy (Greenwood and Hinings, 1993). In most cases, such changes create confusion and uncertainty and produce an environment that lacks norms, templates, and models about appropriate strategies and structures (New-

man, 2000). A lack of regulatory templates is reflected in substantively inconsistent responses of major SM companies to law enforcement requests. Hoover (2010) summarizes the FBI's experiences in dealing with the top three social networking sites:

> *……Facebook is "often cooperative" with law enforcement emergency requests for information, while MySpace requires law enforcement to provide a search warrant to see private messages less than 181 days old. Twitter, meanwhile, is apparently even less helpful than MySpace, as the presentation notes it has no contact number for law enforcement to call, only retains the last log-in IP address, has no guide for law enforcement, and will not produce data without a warrant or subpoena.*

Normative Institutions

Lack of ethical and professional guidelines

Cisco chief security officer John N. Stewart observed that organizations tend to be slower in the introduction of data integrity policies compared to consumers' adoption of new technology (The Straits Times, 2010). The same is true of professional associations. Professional and ethical guidelines regarding posts on social networking have not been well-developed. In the medical world, for instance, there arguably is a lack of clear guidelines as to what constitutes an unethical or unprofessional online conduct for physicians (Lagu, Kaufman and Asch, 2004; Thompson, Dawson and Ferdig, 2008).

Illegal or questionable activities such as violation of patient confidentiality are taking place in the social networking sites without the violators' intent. In a survey conducted among U.S. medical schools to assess professionalism in medical students' online posts, 60% of the respondents reported incidents of their medical students posting online content that were unprofessional and 13% violated patient confidentiality. The study also found that only few schools had policies to deal with such violations. Illegal or questionable activities (such as, violation of patient confidentiality) are taking place in the social networking sites without the violators' knowledge or intent (Chretien, Ryan, Chretien and Kind, 2009).

Many app developers have also failed to follow ethical guidelines and principles. The Hong Kong-based developer, Pencake had developed the popular "Create Your Quiz" app, which was Facebook's No. 3 most popular outside developer behind Zynga and Electronic Arts. In July 2010, Facebook announced that it disabled Pencake's apps because Pencake had allegedly violated the "main principles" of Facebook's platform policies and codes of ethics. Facebook's code of ethics requires that a user must not spam or infringe on members' privacy.

We cannot really take the deletion of a single developer's apps as "proof positive" that SM providers, such as Facebook, may be serious about ensuring security and privacy of users' information. Cowan (2010) argues: "[w]hile Facebook doesn't sell users' information to advertisers, it remains unclear what happens to the personal data harvested by the dozens of games, quizzes, personality tests and other time wasters that clutter Facebook".

Prior researchers have suggested that less visible players (e.g., independent developers) are more likely to engage in unethical and even illegal practices compared to more visible players (e.g., Facebook). Why might this be the case? For one thing, less visible players are less likely to be spotlighted by the media. To examine why firms show a differential tendency to engage in and respond to potentially demeaning and reputation-damaging activities (e.g., violating SM users' privacy and engaging in fraudulent activities) it would be helpful to consider the stigmatization process associated with such activities. A central concept here is arbiters. Note that arbiters' views and/or actions have influence over social behavior.

Wiesenfeld, Wurthmann, and Hambrick (2008) argue that arbiters' "constituent-minded sensemaking" influences the stigmatization process. They have identified three categories of "arbiters"—social, legal, and economic. Social arbiters include members of the press, governance watchdog groups, academics,

and activists. Legal arbiters are those who enforce rules and regulations. Economic arbiters make decisions about engaging in economic exchange with individuals.

News media reports serve as an intermediary affecting the perceptions of the market audience about a firm's scandalous and "nonconforming" behaviors (Rindova, Pollock, and Hayward, 2006). Media reports have also played a critical role in the criminalization of computer crimes (Hollinger and Lanza-Kaduce, 1988). Prior research indicates that the extent to which arbiters and other external actors criticize, devalue, or question a firm (following a reputation-damaging event) is a function of the firm's external visibility and reputation (Rhee and Valdez, 2009). In the automobile industry, for instance, media are more likely to target and write negative comments on recalls by higher reputation automakers than on the lower reputation automakers (Haunschild and Rhee, 2004; Rhee and Haunschild, 2006). Consistent with theory, SM actors with a higher degree of external visibility seem to experience more scrutiny and direct more efforts toward preventing privacy and security breaches.

In April 2010, four U.S. Senators argued that Facebook needed to enhance privacy measures (Liedtke, 2010). The Electronic Privacy Information Centre and 15 other groups filed a complaint about Facebook's instant personalization with the Federal Trade Commission in May 2010 (Cowan, 2010). The Federal Trade Commission examined the privacy and data collection practices of social networking sites including Facebook (Liedtke, 2010). Likewise, in March 2010, Jim Gamble, chief executive of the Child Exploitation and Online Protection (CEOP) criticized Facebook after investigators found that a convicted murderer met his teenage victim through a fake Facebook profile (Belfast Telegraph, 2010).

Facebook and other SM sites responded by announcing some security measures. For instance, Bebo and Facebook introduced the safety application ClickCEOP. ClickCEOP buttons were developed to protect users under 18 from cyber-bullies and other abuses. That may be a small comfort for Facebook users', parents. Likewise, Facebook Beacon, which allowed sharing users' activity on third-party sites (e.g., eBay and Fandango) with friends was modified following complaints from users and privacy advocacy groups (Fletcher and Ford, 2010).

Cognitive Institutions

The institutions associated with cognitive programs are built on mental maps of individual users and thus function primarily at the individual level (Huff, 1990). Many effects can serve as cognitive feedback depending on the nature and motivation of the actor. Put differently, cognitive systems influence the lens through which users view the risks involved in SM (Scott, 2001). SM users' skills, expertise, experience, knowledge, and technical know-how can be considered as components of interest for cognitive institutions.

Precautionary measures

Most SM users are found to perform poorly in risk assessment exercises involving their information online. The Australian Federal Police AFP's high tech crime group recently conducted a trial among a group of Facebook users and found that 98 % of them had put enough information on their personal pages to allow identities to be stolen (Neighbour, 2010). Similarly, Sophos' study conducted in 2008 found that 40% of Internet users used the same password for all websites they accessed (Miller and Stone, 2009). According to Consumer Reports' State of the Net survey released in May 2010, 3% of SM users admitted mentioning when they were away from home, 52% posted their full birth date, information 21% posted photos of children, 13% posted children's names and 8% provided home street address (Woollacott, 2010). Note too that according to Britain's fraud prevention agency, Cifas a recent trend has been the rise in identity fraud which makes use of the victim's current address (Salmon, 2010).

Experts argue that employers should avoid encouraging untrained and unmonitored employees to blog about their company's prod-

ucts and services. This is especially important if an employer is concerned about its goodwill or it recognizes that SM may have a potential to expose private company practices that can be perceived as unfair or deceptive (Lazar, 2010). Professional service organizations, comprising highly trained and licensed professionals such as physicians, radiologists and lawyers--known as "extreme" professional services, extensively rely on tacit knowledge and long training periods (Levy, Goelman, Yu and Paging, 2006; Levy and Yu, 2006; Singh and Wachter, 2008). These organizations are greatly concerned about security issues associated with SM . Boston Medical Center (BMC), a private hospital center affiliated with Boston University, offers a case in point. BMC blocks access to all SM websites using security software from Websense Inc. Users who attempt to access SM sites such as Facebook, YouTube or Twitter are shown a page indicating that their destination is off-limits. Brad Blake, director of IT at BMC noted that if BMC employees created a Facebook account and patients to be friends, "that would constitute a security breach". He went on saying that "[o]ur senior management has felt it easier just to block these sites rather than trying to police and manage them" (Tucci, 2010).

A failure to understand the context of SM use is also likely to lead to an exposé of potentially unethical and even illegal behaviors and practices. For instance, in 2009, a Facebook profile led to a cancellation of a Canadian woman's disability payments by her insurance company. The reason was that her profile on social networking sites claimed she was no longer depressed. The insurance company said it had seen photos of the woman on Facebook, enjoying herself on nights out and on a beach vacation (Cross, 2009).

A final point is that younger SM users perform poorly on precautionary measures compared to older ones. For instance, a study found that 22% of all Internet users made five or more pieces of personal information (e.g., birth date, home address, cellphone number) available on their social networking pages. The proportion was 32% for people between the ages of 18 and 32 (Cowan, 2010).

Defensive measures

An understanding of manipulative techniques used by various creatures to fool their enemies is of particular relevance for cybercrimes involving SM. In particular, a phenomenon proposed by Dawkins (1982) called the "rare enemy syndrome," provides a helpful theoretical perspective for understanding how victims often fall to new unfamiliar baits or lures. The basic idea behind rare enemy syndrome is simple. The enemy's manipulation is so rare that evolutionary development has not yet progressed to the point that the victim has an effective counter poison (de Jong, 2001).

From the potential victim's standpoint, one important point to note about social networking is that most SM users are young. For instance, while 52% of the population in Singapore used SM in 2010, the proportions were 95% for the 15-19 age-group and 89% for the 20-29 age-group (Supreme Court of Singapore, 2010). In this regard, the teens' and youth's cognitive skills and competencies, and, associated beliefs are considered as major influencing factors on their SM behaviors and outcome. According to a recent study, 42% of respondents in the 18 to 29 age groups were unable to answer any question about privacy law correctly (Cowan, 2010). Cyber-criminals preying on them can be considered as the "rare enemy" since youths and teens haven't yet developed counterpoison to deal with them.

A parallel can be drawn from the literature on physical crimes. Most cyber-criminals that prey upon SM users employ a similar modus operandi as in physical crimes which involve gaining access to and trust of the victim. The victimization process can viewed as a temporal sequence of activities through which the crime progresses. For instance, offenders against children (such as, pedophiles) usually use the power of persuasion and friendship to first gain the trust of the child, and in some cases parents, as well. Friendship is a critical step toward gaining cooperation (Elliott, Browne and Kilcoyne, 1995; Leclerc, Beaure-

gard and Proulx, 2008; Murray, 2000). We would argue that fraudsters find it easy to gain trust and cooperation of SM users who have no past experience of distrust. One online romance scam victim, Sally Schrock reported that a scammer she met on a social networking site started sending her gifts (gaining trust) (kmbc.com, 2006). The scammer then asked for her Social Security number and e-mail password (gaining cooperation).

Additionally, part of the fascinating character of social networks stems from the fact that they are built on trust-based architectures. The real or perceived relationships of trust that connect social networking users increase scammers' chance of gaining trust and cooperation from potential victims. For, for example, a fraudulent message sent from a SM user's social network is often considered to be more trustworthy compared to random a spam message (Ramsey and Venkatesan, 2010).

Discussion and Implications

SM providers are pushing their users a bit too hard to share personal information. A convenient but possibly false assumption among some SM providers is that the Internet generation values openness and cares less about privacy (Cowan, 2010). In April 2010, Facebook came up with new rules, which required members to share more information (Lyons, 2010).

One way to understand SM providers' orientation towards security and privacy would be to examine them in the backdrop of current institutional arrangements and technological development. For SM providers (such as, Facebook) to maintain control over various actors (e.g., consumers, advertisers, regulators and privacy advocacy groups), a proper decoupling of responses is needed. Decision makers in social networking sites simultaneously utilize different combinations of actions in parallel that reflect their mixed reading of the environment (George, Chattopadhyay, Sitkin and Barden, 2006).Various institutional actors differ in terms of power they have to affect an organization's (e.g., Facebook's) outcome. Different theoretical contributions and various empirical studies have led to the accepted view that the exact nature of decoupling is a function of relative powers of competing organizational and institutional interests (March and Olsen, 1989; Oliver, 1991; Pfeffer, 1981a, b; Westphal and Zajac, 1994, 1998, 2001; Zajac and Westphal, 1995). These studies also provide support for the notion that substantial responses cannot be made to appease two sets of actors that diametrically oppose one another. More to the point, the substantive response relates to the threat or opportunity associated with the actor that is perceived to be more powerful and the symbolic response relates to the threat or opportunity associated with the actor perceived to possess less power (George, Chattopadhyay, Sitkin, and Barden, 2006).

Facebook's substantive response relates to the advertising opportunity. That is, advertisers are more powerful actors than consumers from the company's standpoint. A Newsweek article asserted (Lyons, 2010):

> *The truth is, Zuckerberg [Facebook founder and CEO] needs your data. His business is built on it. You are not Facebook's customer. You are its inventory--you are the product Facebook is selling. Facebook's real customers are advertisers. You're useful only because you can be packaged and sold. The more information Facebook extracts from you, the more you are worth. Consider that in 2005, Facebook's privacy policy was one sentence long and said that none of your info would be shared with anyone who wasn't in one of your groups. Today the policy is longer than the Constitution and requires a lawyer to parse its meaning. Why doesn't Facebook just use its original one-sentence policy? I'll take a wild guess and say advertisers, not members, were the driving force here.*

As to the involvement of the third party developer in the value chain, it is worth noting that an innovation's success hinges on having well-developed systems and components that are interoperable and compatible with a company's products and the creation of externalities. Such products help create a promising innovation ecosystems–"the collaborative ar-

rangements through which firms combine their individual offerings into a coherent, customer-facing solution" (Adner, 2006).

A final observation is that the widespread use of social networking platforms can be considered as a part of a more general trend toward cloud computing (Ramsey and Venkatesan, 2010). In this regard, various security risks and challenges associated with cloud computing deserve attention (Kshetri, 2010b, 2011).

Managerial Implications

Our account has implications for management practices. In light of the lack of well-developed institutional frameworks such as regulations, and ethical and professional standards, there is a strong need for organizations to develop policies, culture and techniques to manage and monitor SM uses within an organization. Organizations that have clear policy, procedures, limits, and instructions regarding the use of SM are less likely to become targets or victims of various forms of cybercrimes. For instance, as noted above, apps downloaded from less reputed websites are more likely to pose security risks. In this regard, organizations need to have a clear policy regarding apps download in devices owned by the organization. For instance, some online game apps may not only lead to a decline in employee performance but also to an increased security risk.

In light of organizations' use of SM in diverse activities, it is also important to have clear policies and guidelines regarding posts on SM networks by employees. It may also be important to regularly monitor online posts on SM sites by employees, which may lead to a leak of organizational secrets. This is especially important for organization dealing with sensitive information such as hospitals and government departments.

From organizations' standpoint, criminal activities of various cybercrime firms are not the only risks associated with SM. Sometimes organizations are likely to become targets and victims of unfair and unjust criticisms that are raised by various stakeholders through social media campaigns. In such cases, organizations can use SM to defend themselves against unjust criticisms from these campaigners. That is, just like diamond is the only material hard enough to cut diamond effectively, SM can be an effective tool to fight against a social media campaign targeted against a company. A nice and striking example to illustrate this point would be Procter & Gamble's (P&G) use of social media to address concerns of a group of consumers that were dissatisfied with its Dry Max technology, who initiated a Facebook campaign against the technology. In 2009, P&G introduced the technology into its Pampers product line, which also received awards from parenting magazines (Heussner, 2010). A customer reported that her child had developed a diaper rash, who created a Facebook page in an attempt force P&G to withdraw the product. By May 2010, 7,000 parents had joined the anti-Dry Max campaign, which created intense pressures on the firm to withdraw the product from the market (Barwise and Seán, 2010). P&G was, however, confident in Dry Max's performance thanks to its long experience in such products. The company's experience was that some proportions of babies always develop rashes. P&G's well-established SM networks such as Pampers Village and Pampers Facebook page proved to be highly effective to fight against the anti-Dry Max campaign. Through these platforms, P&G made its case sympathetically, clearly and authoritatively. The company responded to all complaints, offered advices, and explained compelling reasons as to why the product would not be withdrawn. A September 2010 report of the U.S. Consumer Product Safety Commission indicated that the agency found no link between Dry Max and the occurrence of diaper rash.

Concluding Comments

Management of security risks is a critical practical challenge that organizations face in the digital economy. The above analysis indicates that the SM security and privacy challenges are significant. Social networking sites are a potential goldmine for cyber-criminals. It is clear from the privacy and security approaches of SM providers that they have lost

sight of what had made them great. Most SM users, on the other hand, lack precautionary measures in their SM activities. There has also been a lack of defensive measures or counterpoison.

Ensuring that both technological and behavioral/perceptual factors are given equal consideration in the design and implementation of a computer network is thus crucial. Technological measures range from simply disconnecting databases containing sensitive information from the Internet to the deployment of sophisticated anti-fraud technologies. Similarly, simple behavioral measures can stop some serious cybercrimes. A simple training strategy aimed at improving the ability of employees to use SM more securely is likely to reduce a significant proportion of cybercrimes.

Finally, today, there is an emerging trend toward the use of contents posted on social media as evidence in civil and criminal proceedings (Supreme Court of Singapore, 2010). This trend is likely to affect the naïve (e.g. youths and teens) more than the general population. The above discussion also indicates that a failure to understand the context of SM use is also likely to lead to an exposé of wrongdoing.

Acknowledgements

The author is grateful to Dr. T.P. Liang, PA-JAIS Editor in Chief and the reviewers for their insightful comments, which helped to improve this paper substantially.

Footnotes

[1] Here is how click fraud on Facebook works. A fraudster may use fake accounts logs in to Facebook and views the ads that are displayed. When a competitor's ads are displayed, the fraudster clicks them. Note that, according to Facebook rules, up to six clicks on an ad by a user in a 24 hour period are charged to the advertiser (Techcrunch.com 2009). Fraudsters reportedly create thousands of fake Facebook accounts with a wide variety of demographic information. One advertiser reportedly paid $200 to an Indian operation for 2,000 Facebook accounts. The going rate was $10 per 100 accounts if unique email accounts are supplied. Once the accounts are created, they use software to fill out the varied demographic information, and that software also manages all these accounts (Techcrunch.com 2009).

[2] The concept of manifest and latent functions (Merton 1968) can be very helpful in understanding astroturfers' behaviors. Manifest functions are explicitly stated and understood by the participants in the relevant action and the consequences can be observed or expected. Latent functions are those that are not explicitly stated or recognized by the people involved. In a SM campaign, for instance, the manifest posture is bloggers' testimonials about certain brands, but below the surface deeply ingrained are various actions orchestrated by Astroturfers.

References

Adner, R. (2006). "Match your innovation strategy to your innovation ecosystem," *Harvard Business Review*, 84 (4), 98-107.

Arrington, M.(2009). "Facebook Click Fraud 101," http://techcrunch.com/2009/06/26/facebook-click-fraud-101. Accessed on June 26, 2009.

Audretsch, D. B. (1991). "New Firm Survival and the Technological Regime," *Review of Economics and Statistics*, 73, 441-450.

Barwise, P. and Meehan, S. (2010). "The One Thing You Must Get Right When Building a Brand," *Harvard Business Review*, 88(12), 80-84.

Belfast Telegraph.(2010). "Facebook's new child safety link welcomed," 12, July 12.

Brenner, S. W. (2004). "Toward a criminal law for cyberspace: A new model of law enforcement?," *Rutgers Computer and Technology Law Journal*, 30, 1-9.

Campbell, J. L. (2004) *Institutional Change and Globalization*. Princeton, New Jersey: Princeton University Press.

Chen, S. (2010). "Workplace rants on social media are headache for companies," Retrieved from

http://www.cnn.com/2010/LIVING/05/12/social.media.work.rants/index.html on May 12, 2010.

Chretien, K. C., Ryan, G. S., Chretien J. P. and Kind, T. (2009). "Online Posting of Unprofessional Content by Medical Students," *JAMA*, 302, 12, 1309-1315.

Christian Science Monitor. (2006). "When The Law Chases The Internet," 98, 77, March 17, 6.

Clarke, R. V. (1995). "Situational crime prevention," In M. Tonry & D. P. Farrington (eds.), *Building A Safer Society: Strategic Approaches To Crime*, Chicago: University of Chicago Press, 91–150.

Cooter, M. (2011). "Facebook Most Often Blocked by Businesses," January 24, Retrieved from http://www.pcworld.com/article/217503/facebook_most_often_blocked_by_businesses.html on September 18, 2010.

Cowan, J. (2010). "Why We'll Never Escape Facebook," *Canadian Business*, 83(10), 28-32.

Cross, A. (2009). "Know your enemies? Know your friends; Social media scams: Privacy breaches affect relationships as well as wallets, professor says," *The Gazette (Montreal)*, p. B2.

Cutler, K. and Marshal, M. (2009). "Facebook's self-serve ads "crushing it," help turn startup cash-flow positive," Retrieved from http://digital.venturebeat.com/2009/09/18/facebooks-self-serve-ads-crushing-it-lead-to-profitability on September 18, 2009.

Dawkins, R. (1982).*The extended phenotype*. Oxford University Press, New York.

De Jong, W. M. (2001). "Manipulative tactics in budgetary games: The art and craft of getting the money you don't deserve," *Knowledge, Technology & Policy*, 14(1), 50–66.

Dickson, M., BeShers, R. and Gupta, V. (2004). "The impact of societal culture and industry on organizational culture: Theoretical explanations," In J. H. Robert, J. H. Paul, J. Mansour, W. D. Peter, and G. Vipin (eds). *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*, Thousand Oaks, Calif: Sage Publications.

Elliott, M., Browne, K. D. and Kilcoyne, J. (1995). "Child sexual abuse prevention: What offenders tell us," *Child Abuse & Neglect*, 5, 579-594.

Finkle, J. (2009). "The Globe and Mail (Canada) Friend or cyber criminal? Cybercrime growing on Facebook," *Reuters*, July, L3.

Fletcher, D. and Ford, A. (2010). "Friends without Borders," *Time*, 175 (21), May 31, 32-38.

Foreign.peacefmonline.com. (2010). "Why a top Facebook app maker vanished," Retrieved from http://foreign.peacefmonline.com/news/201007/64491.php on July 29, 2010.

George, E., Chattopadhyay, P., Sitkin, S. B. and Barden, J. (2006). "Cognitive underpinnings of institutional persistence and change: A framing perspective," *Academy of Management Review*, 31(2), 347-385.

Glaser, D. (1971). *Social deviance*. Chicago, IL: Markham.

Gordon, S. and Ford, R. (2006). "On the definition and classification of cybercrime," *Journal in Computer Virology*, 2, 13–20.

Greenwood, R. and Hinings, C. R. (1993). "Understanding strategic change: The contribution of archetypes," *Academy of Management Journal*, 36, 1052-1081.

Haunschild, P. R. and Rhee, M. (2004). "The role of volition in organizational learning: The case of automotive product

recalls," *Management Science*, 50, 1545–1560.

Heussner, K. M. (2010). "Parents Protest New Pampers Diapers on Facebook," Retrieved from http://abcnews.go.com/Technology/parents-protest-pampers-diapers-facebook/story?id=10537369 on July 22, 2011.

Hollinger, R. and Lanza-Kaduce, L. (1988). "The Process of Criminalization: The Case of Computer Crime Laws," *Criminology*, 26, 101-126.

Hoover, J. N. (2010). "FBI Goes Undercover on Social Networks," *InformationWeek Magazine*. Retrieved from http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=223900114 on March 16, 2010.

Huff, A. S. (1990). "Mapping strategic thought," In A. S. Huff (ed.). *Mapping strategic thought*. Chichester, England: Wiley, pp. 11-49.

Kaplan, M. (2009), "Caution in cyberspace," *Sunday Tasmanian (Australia)*, May, Edition 1, p. 8.

Katyal, N. K. (2001). "Criminal law in cyberspace," *University of Pennsylvania Law Review*, 149(4), 1003–1114.

Kavur, J. (2010). "Social media isn't friends with enterprise security," Retrieved from http://www.networkworld.com/news/2010/041410-social-media-isnt-friends-with.html?page=1 on April 14, 2010.

Kee, T. (2009). "The Feds to Push For 'Truth' In Social-Media Marketing," Retrieved from http://www.forbes.com/2009/04/03/truth-in-social-media-marketing-technology-paidcontent.html on April 3, 2009.

Keizer, G. (2006). "Cybercrime Feared 3 Times More Than Physical Crime," *InformationWeek*, January 25.

kmbc.com (2006). "Online Romance Scams Continue to Grow," Retrieved from http://www.kmbc.com/r/9246998/detail.html on May 19, 2006.

Kowalski, M. (2010). "Singapore studies social media use in litigation," Retrieved from http://business.financialpost.com/2010/08/23/singapore-studies-social-media-use-in-litigation on August 23, 2010.

Kshetri, N. (2010a). *The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives*. New York, Berlin and Heidelberg: Springer-Verlag.

Kshetri, N. (2010b). "Cloud Computing in Developing Economies," *IEEE Computer*, 43(10), 47-55.

Kshetri, N. (2011). "Cloud Computing in the Global South: Drivers, Effects and Policy Measures," *Third World Quarterly*, 32(6), 995-1012.

Lagu, T., Kaufman, E. J. and Asch, D. A. (2010). "Armstrong, K. Content of weblogs written by health professionals," *J Gen Intern Med*, 23, 10, 1642-1646.

Lardinois, F. (2009). "63% of Businesses Fear That Social Networking Endangers their Corporate Security," Retrieved from http://www.readwriteweb.com/archives/businesses_fear_social_networking.php on April 28, 2009.

Lazar, B. (2010). "Drafting Social Networking Policies," *Information Today*, 27(5), 20.

Leclerc, B., Beauregard, E. and Proulx, J. (2008). "Modus operandi and situational aspects in adolescent sexual offenses against children: a further examination," *Int J Offender Ther Comp Criminol*. 52 (1),46-61.

Levy, F., Goelman, A., Yu, K. H. and Paging, G. (2006). "Radiology as a case study

in sending skilled jobs offshore," *Milken Institute Review*, 2nd Qtr, 64-72.

Levy, F. and Yu, K. (2006). "Off-shoring Radiology Services to India," September. Working paper, The Industrial Performance Center (IPC) is an MIT, MIT-IPC-06-005.

Liedtke, M. (2010). "Senator urges Facebook founder to improve privacy controls," Retrieved from http://www.boston.com/business/technology/articles/2010/04/28/senator_urges_facebook_founder_to_improve_privacy_controls on April 28, 2010.

Lyons, D. (2010) "Facebook's False Contrition," *Newsweek*, 155(23), June 20.

Magder, J. (2010). "Companies cracking down on Facebook, Twitter in the workplace," Retrieved from http://www.montrealgazette.com/business/Companies+cracking+down+Facebook+Twitter+workplace/2934691/story.html on April 21, 2010.

March, J. G. and Olsen, J. P. (1989). *Rediscovering Institutions. The Organizational Basis of Politics*, New York: Free Press.

Marks, P. (2010)."Social networks must heed the human element," *New Scientist*, 206, 2763 June, p. 19.

McArthur, R. (2010). "Extortion via Facebook on the rise in the UAE," http://www.emirates247.com/news/emirates/extortion-via-facebook-on-the-rise-in-the-uae-2010-08-21-1.281729. Accessed on August 21, 2010.

Merton, R. (1968). *Social theory and social structure*. New York: Free Press.

Miller, C. C. and Stone, B. (2009). "Breached e-mail accounts raise 'cloud computing' security concerns," *The International Herald Tribune*, July, 15.

Morrissey, B. (2010). "Value of a 'Fan' on Social Media: $3.60: The findings are based on impressions generated in Facebook's news feed," Adweek, Retrieved from http://www.adweek.com/aw/content_display/news/digital/e3iaf69ea6718351232f8a0f92213b59293 on April 13, 2010.

Murray, J. B. (2000). "Psychological profile of pedophiles and child molesters," *J Psychol*, 134, 211-224.

Naylor, R. T. (2005) "The Rise and Fall of the Underground Economy," *Brown Journal of World Affairs*, 11(2), 131-143.

Neighbour, S. (2010) "Terror moves into the digital age," *The Australian*, (March 2010), All-round Country Edition, 13.

Newman, K. L. (2000) "Organizational transformation during institutional upheaval," *The Academy of Management Review*, 25(3),602-619.

Nielsen.com. (2010). "Social Media Dominates Asia Pacific Internet Usage," http://blog.nielsen.com/nielsenwire/global/social-media-dominates-asia-pacific-internet-usage. Accessed on July 9, 2010.

North, D. C. (1990). *Institutions, institutional change and economic performance*. Cambridge, MA: Harvard University Press.

North, D. C. (1996). "Epilogue: Economic Performance Through Time," In L. J. Alston, T. Eggertsson, and D. C. North (eds.). *Empirical Studies in Institutional Change*. Cambridge: Cambridge University Press,342-355.

Null, C. (2001). "How To Avoid Facebook & Twitter Disasters," *PC World*, 27(8),97-103.

Oliver, C. (1991). "Strategic Responses to Institutional Processes," *Academy of Management Review*, 16, 145–179.

Pepitone, J. (2010). "Facebook hits 500 million users," Retrieved from http://money.cnn.com/2010/07/21/technolo-

gy/facebook_500_million/index.htm on July 22, 2010.

Peppiatt, R. (2010). "Crimes on Facebook Rise 346%," *Daily Star*, April 3, U.K. 1st Edition, 14.

Pert, J. (2010). "Facebook Security Warning: Dislike Button is a Scam," Retrieved from http://www.product-reviews.net/2010/08/17/facebook-security-warning-dislike-button-is-a-scam on August 17, 2010.

Pfeffer, J. (1981a*)* Management as symbolic action. *Research in Organizational Behavior*, 3, 1-52.

Pfeffer, J. (1981b*) Power in Organizations*, Marshfield, MA: Pitman.

Ramsey, G. and Venkatesan, S. (2010). "Cybercrime Strategy for Social Networking and Other Online Platforms," *Licensing Journal*, 30, 7, 23-27.

Rhee, M. and Haunschild, P. R. (2006). "The liability of good reputation: A study of product recalls in the U.S. automobile industry," *Organization Science*, 17, 101–117.

Rhee, M. and Valdez, M. E. (2009). "Contextual Factors Surrounding Reputation Damage With Potential Implications For Reputation Repair," *Academy of Management Review*, 34(1), 146-168.

Richmond, R. (2010). "Facebook Moves to Thwart Cybercrooks," Retrieved from http://gadgetwise.blogs.nytimes.com/2010/05/13/facebook-moves-to-thwart-cybercrooks on May 13, 2010.

Rindova, V. P., Pollock, T. G. and Hayward, M. L. A. (2006). "Celebrity firms: The social construction of market popularity," *Academy of Management Review*, 31, 50–71.

Rodgers, W. (2009). "Cyberattacks: Can Google – or Uncle Sam – protect you?," *Christian Science Monitor*, April, pN.PAG.

Salmon, J. (2010). "Warning as bank card fraud soars," Retrieved from http://www.thisismoney.co.uk/credit-and-loans/id-fraud/article.html?in_article_id=503831&in_page_id=159&expand=true on May 4, 2010.

Scott, W. R., Ruef, M., Mendel, P. J. and Caronna, C. A. (2000). Institutional Change and Healthcare Organizations: From Professional Dominance to Managed Care. Chicago: University of Chicago Press.

Scott, W. R. (2001). *Institutions and organizations*. Thousand Oaks, CA: Sage.

Singh, S. N. and Wachter, R. M. (2008). "Perspectives on Medical Outsourcing and Telemedicine – Rough Edges in a Flat World?," *The New England Journal of Medicine*, 354, 1622-1627.

Softpedia.com (2009). "Facebook Sued in California over Privacy Concerns", August 18, Retrieved from http://news.softpedia.com/news/Facebook-Sued-in-California-over-Privacy-Concerns-119515.shtml on March 28, 2010

Soghoian, C. H. (2008). "Hackers Target Facebook Apps," Retrieved from http://news.cnet.com/8301-13739_3-9904331-46.html on March 28, 2008.

Sullivan, E. A. (2009). "Play by the New Rules," *Marketing News*, 43(19), 5-9.

Supreme Court of Singapore. (2010). Use and Impact of Social Media in Litigation: Consultation Paper**.** Retrieved from http://app.supremecourt.gov.sg/data/doc/ManageHighlights/2586/Public%20Consultation%20Paper%20for%20the%20use%20of%20social%20media%20in%20civil%20litigation.pdf on August 4, 2010.

Tanase, S. (2010). "When Web 2.0 sneezes...everyone gets sick," *Engineering & Technology*, 5, 5, 28-29.

Techcrunch.com. (2009). "Facebook Click Fraud Enraging Advertisers," Retrieved from http://techcrunch.com/2009/06/21/facebook-click-fraud-enraging-advertisers/#ixzz0onAAps6u on June 21, 2009.

The Straits Times (Singapore) (2010). "Productivity takes a hit too," July 29.

The Sydney Morning Herald. (20100. "Facebook hacker claims to be based in NZ," Retrieved from http://news.smh.com.au/breaking-news-world/facebook-hacker-claims-to-be-based-in-nz-20100426-tmx2.html on April 26, 2010.

Thompson, L. A., Dawson K. and Ferdig R. (2008). "The intersection of online social networking with medical professionalism," *J Gen Intern Med*, 23, 7,954-957.

Tuazon, J. and Mark, V. (2010). "Social Media the New Battleground for Spam, Malware: Sophos," Retrieved from http://www.pcworld.com/article/197169/social_media_the_new_battleground_for_spam_malware_sophos.html on May 26, 2010.

Tucci, L. (2010). "CIOs weigh use of social media against security concerns," Retrieved from http://searchcio.techtarget.com/news/article/0,289142,sid182_gci1510466,00.html on April 22,.

Voigt, K. (2009). "Dangerous Internet search terms grow with cybercrime," *CNN.com*, June 21.

Westphal, J. D. and Zajac, E. J. (1994). "Substance and symbolism in CEOs' long-term incentive plans," *Administrative Science Quarterly*, 39,367–390.

Westphal, J. D. and Zajac, E. J. (1998). "The symbolic management of stockholders: Corporate governance reforms and shareholder reactions," *Administrative Science Quarterly*, 43, 127–153.

Westphal, J. D. and Zajac, E. J. (2001). "Explaining institutional decoupling: The case of stock repurchase programs," *Administrative Science Quarterly*, 46, 202–228.

Whitney, L. (2010). "Malware and social network attacks surge in 2009," *CNET News*, Retrieved from http://news.cnet.com/8301-1009_3-10454870-83.html on February 17, 2010.

Wiesenfeld, B. M., Wurthmann, K. A. and Hambrick, D. C. (2008). "The Stigmatization and Devaluation of Elites Associated With Corporate Failures: A Process Model," *Academy of Management Review*, 33(1),231-251.

Woollacott, E. (2010). "Most social network users court cybercrime, says report," http://www.tgdaily.com/security-features/49619-most-social-network-users-court-cybercrime-says-report. Accessed on May 4, 2010.

Zajac, E. J. and Westphal, J. D. (1995). "Accounting for the explanations of CEO compensation: Substance and symbolism," *Administrative Science Quarterly*, 40, 283–308.

Zittrain, J. (2009). "Lost in the Cloud," *The New York Times*, Late Edition – Final, Section A, July 19.

About Authors

Nir Kshetri is Associate Professor at the University of North Carolina-Greensboro and a research fellow at Research Institute for Economics & Business Administration - Kobe University. Nir holds a Ph D in Business Administration from University of Rhode Island. He is the author of Global Entrepreneurship: Environment and Strategy (Routledge: New York), The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives (Springer-Verlag: Berlin, Heidelberg, New York, 2010) and The Rapidly Transforming Chinese High Technology Industry and Market: Institutions, Ingredients, Mechanisms and Modus Operandi (Caas Business School, City of London and Chandos Publishing: Oxford, 2008). Nir has published fifty journal articles in Foreign Policy, European Journal of Marketing, Journal of International Marketing, Third World Quarterly, Journal of International Management, Communications of the ACM, IEEE Computer, IEEE Security and Privacy, IEEE Software, Electronic Markets, Small Business Economics, Thunderbird International Business Review, Telecommunications Policy, Journal of International Entrepreneurship, Electronic Commerce Research and Applications, Baltic Journal of Management, IT Professional, Journal of Health Organization and Management, Journal of Developmental Entrepreneurship, International Journal of Health Care Quality Assurance, Journal of Electronic Commerce Research, and others.