Received for publication: 28.11.2014. Review paper

UDK: 343.9

PHENOMENAL EXPLORATION INTO IMPACT OF ANONYMITY ON LAW AND ORDER IN CYBERSPACE

Xingan Li
Tallinn University Law School

SUMMARY

While information systems provide modern society with great convenience, it also poses new problems in maintaining social order. One of its negative influences is the anonymity of cyberspace, which makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement. The article explores how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, what potentialities the anonymity has, how the trans-territorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

Keywords*: cyber anonymity, dark figure, social order, law enforcement*

INTRODUCTION

The pervasion of information systems facilitates efficient access to information. While privacy is at high risk, anonymity, invisibility, and concealment of criminal traces become issues of broad concerns. The anonymity of cyberspace makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. This article deals with the formation and problem of anonymity in cyberspace in general, and

anonymity of cybercriminals in particular. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement.

Following this section, the article will explore how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, how the anonymity protects cybercriminals, how the trans-territorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

WRESTLING BETWEEN CYBER ANONYMITY AND LAW AND ORDER

Information systems have been increasingly critical in facilitating efficient access to information. Today, approximately 3 billion users, or 42% of the world population (Internet World Stats 2014) entered a new space networked by instant transfer of information. With much more information being accumulated, consumption of information becomes a double-edged process. While there is superfluous spam information, privacy is at high risk. Although people have appreciated the value and significance of cyber anonymity, negative concerns also emerge in anonymity, invisibility, and concealment of criminal traces. Cybercrime differs from traditional crimes in many different ways, including its universality and complexities, in particular, its anonymity, concealment, and invisibilities. The anonymity of cyberspace makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations.

For example, in the case of spam, the e-mail can be both the instrument and the objective that are used in commercial, political, malicious, or illegal schemes. As a marketing and communications means, e-mail has been gradually abused. Unsolicited commercial mails (UCE) are typically sent anonymously or with a fabricated identity, and the recipients cannot discontinue successive messages. Messages of this kind furthermore consist of false or misleading headers, deceiving recipients to retrieve messages that they do not desire. Moreover, the recipients have no technique of expressing their inclination not to

receive such messages, and have no approach of requesting compensation even if they undergo loss. The abuse of e-mail has turned into a public annoyance in the online background. Even if the application of anti-spam services and technologies is escalating, the degree of spam is continuing to boost as swift (OECD 2004, pp. 2-3; OECD 2005, p. 6), becoming a predicament not only for individual e-mail accounts, but also for business accounts.

Another example is cyber terrorism. Despite the fact that cyber terrorism has not developed into a reality as lots of people worried at the end of 20th century, it becomes a gorgeous preference for modern-day terrorists for a number of reasons (Weimann 2004, p. 6). It is cheaper, more anonymous, aiming at a more massive target and number of targets, distantly conducted, and affecting a larger number of people globally. International society has barely implemented any countermeasures against conventional terrorism in the last few years. Weimann claimed that terrorism in cyberspace was more anonymous than conventional terrorist schemes. The fact that terrorists could exploit "screen names" or log on as a "guest user" makes it very difficult for security agencies and police forces to track down their real identity. What made it worse were that in cyberspace there were no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart (ibid., p. 6), making terrorists specially unidentified.

Maybe the most real threats and the most serious worries come from offences such as harassment and murder. In offences where information systems are used as means of committing verbal assault, threat, harassment, alarming, spam and fraud, the motivation of the perpetrator is to harass and to kill the victim. The function of the Internet as a means of communications and with a high anonymity of interaction often entraps the victims into unforeseeable dangers. In 2005, China Ministry of Public Security investigated 1,000 assassination cases, in many of which the criminals found the potential victims through the Internet (Yi 2006). In many criminal cases, stalkers and murderers find, follow, entice, and intimidate victims through the communication and interaction of various Internet services, usually anonymously.

On the other hand, concerning the legal status of cyber anonymity, people have long been disputing in vain. Conventional countermeasures and theories about crime

prevention were based on its material influence and on the material environment, although non-material factors have long existed, too. Activities in information systems can be expressed in a physically invisible form. What are physically visible in information systems are those physical existences, such as hosts and terminals, displayers, keyboards, mouse, and cables, while the mechanisms by which the computers function are invisible. Cyberspace is developed from information systems as an abstract space, differing from the material devices of information systems that include terminals and cables. It is invisible and intangible if compared with traditional space (Khosrow-Pour 1998, p. 440; Robertson 2000, p. 248; Dodge and Kitchin 2001, p. 81). When a web page is surfed, what can be seen is only the display of information on the screen. The web site is not physically a reading room where people can read magazines, newspapers and books, listen to audio records or watch videos, nor a marketplace, bank, street, or forum. It is merely a collection of web pages written in various mark-up languages, comprised of letters, numbers, and symbols in common use, but which facilitate the functions of linkage to other media, communicating with other people or directing to other services. The electronic address is not necessarily located along a street, in a building or even in a city, province, or country. In addition, the online services are usually provided in the manner of a remote transaction paid by means of digital cash or virtual money. Finally, the Internet users include individuals and institutions, but they do not necessarily appear in person or in an entity in a traditional library, forum, marketplace, bank, or along a street. It is entirely an invisible community in an invisible space—a group of anonymous netizens interact behind curtains or masks.

The invisibility of cyberspace worsens the situation caused by cyber anonymity, in the sense that criminals and offences in cyberspace become more concealed, while criminal justice faces greater difficulties.

ANONYMITY SYMBOLIZES CYBERSPACE

The disappearance of physicality in activities on the Internet symbolizes the new way for daily routines, and presents a chance for new practice and changes in faiths, positions, and manners (Zigrus 2001, p. 171). To a certain extent, Internet services are provided for

every user who owns a computer and a modem or cable linked to the server. The real identity of the user is not necessary for using the Internet. That is to say, a high degree of anonymity is achievable. Anonymity could indicate an intention to lie or not, to do something deceit or not. In the environment of online communications, particularly during interaction between remote strangers, information systems provide the possibility of maintaining anonymity, and we found that the users of information systems have the willingness to stay passively anonymous, not necessarily actively lying to their counterparts.

In the case of e-mail, it is uncomplicated to register an e-mail account with false information, or to send messages in the name of a certain person. These e-mails may not only infringe the legal rights and interests of the person of the counterfeited identity, but also are able to fabricate a rumour, slander other people, harm other people's reputation, or practise unfair competition to reduce the competitor's trustworthiness. No obligation of free e-mail service providers has been established to investigate the registrants' identity information. In addition, some web sites also provide anonymous e-mail services or sell anonymous e-mail software (Examples of such services and software can be searched out with search engines). Under such circumstances, the traceback of the real sender is impossible. Only where the providers' status is clear, under vicarious liability, can it be useful for law enforcement in some jurisdictions to hold the re-publisher responsible for the content of the original author (Edwards and Walde, eds. 1997, Part 4). E-mail has frequently been abused in an anonymous manner so as to realize a fraudulent scheme. This anonymity not only facilitates a lie, but may also support a fraud. In R. v. Mastronardi (2006 BCSC 1681), the accused, met the plaintiffs through an Internet dating service, during which the accused misrepresented himself as a single person and engaged in relationship with several victims. He represented himself as:

"(a) coming from a large, powerful and wealthy Sicilian family;

(b) being a widower seeking a wife;

(c) being a medical doctor with a specialty in gynaecology;

(d) having hospital privileges and a clinic;

(e) being a kind, caring and considerate person with positive family and moral beliefs, conveyed in conversations that went on for hours on end;

(f) having elaborate and sometimes bizarre family and cultural traditions requiring highly submissive wives and amalgamation of finances to an account controlled by him;

(g) as time went on, being third in command in mafia like family organization;

(h) not wanting to date, but wanting to immediately enter into an intimate relationship, after which his culture and family regarded them as married;

(i) once so married, his family required him to follow family and cultural traditions." (paragraph 4)

In R. v. Farkas, the accused engaged in online fraud by using different e-mail addresses, mailing addresses, and user names, victimizing sellers and purchasers distributed in the U. S., Canada, and England (2006 ONCJ 121, 10 April 2006). In R. v. Reynolds & Ors, the accused engaged in online chat claiming himself to be a 16-year-old boy, attempting to make young girls expose their bodies and transmit photographs to him over the Internet ([2007] EWCA Crim 538 (08 March 2007)).

There are many ways by which people make efforts to detect lies, usually including various clues to emotion that may disclose the situation of lying (Ekman 1992, as cited in Howitt 2002, pp. 251-253). However, in the electronic lie, none of the clues can be useful, particularly those emotional ones, because there is no face-to-face interaction. Rather, the interaction itself is covered by a human-machine-human fig leaf.

Another field where people usually maintain anonymity is interaction in chat rooms. Accounting for a considerable fraction of the income of the commercial online providers, chat systems support synchronous communication, discussion on different topics, trans-territorial relationships on common interests, and ignorance of social status (Internet Crime Forum IRC subgroup 2001, pp. 7-9; Rowland 1998; Wilbur 1997, p. 5.). The biggest advantage of the interaction in chat rooms is that the user can keep anonymous at the beginning of the chat or remain anonymous during the whole process. Keeping anonymous means that people are able to fabricate identities that cannot be used to identify them. By disguising themselves, users can perpetrate fraud and many other related activities. This approach is definitely useful, too, in detection and investigation of crimes, where law enforcement uses falsified identity to allure and arrest suspects. For example, in United States v. Helder, (Eighth Circuit, No. 05-3387, 16 March 2006), an

undercover officer used a screen name and claimed to be a 14-year-old girl to entrap the perpetrator (pp. 2-4); in United States v. Baker (Seventh Circuit, No. 05-2499, 24 January 2006), an undercover officer used a screen name and claimed to be a 14-year-old boy to entrap the perpetrator (pp. 2-3); in United States v. Antelope (Ninth Circuit No. 03-30557, 8 June, 2004. Docket num. 03-30334, January 2005), the accused joined an Internet site advertising "Preteen Nude Sex Pics" and started corresponding with an undercover law-enforcement agent, in respect of whom the accused was entrapped when he ordered a child pornography video over the Internet; in United States v. McGraw (Tenth Circuit No. 02-1407, D. C. No. 01-CR-426-B, 2 December 2003), the accused was also caught by an undercover agent, with whom he expressed his interests in "having sexual contact with 'white males between the ages of 12 and 15'," and arranged a encounter (See also R. v. Randall, Provincial Court of Nova Scotia 2006 NSPC 19, No. 1538177, 28 April 2006). The actual reality is that, in information systems, determining users' identity proves difficult, but not impossible.

POTENTIALITY OF ANONYMITY

Communicating anonymously is a great characteristic of the Internet environment. In using the Internet, anonymity can be kept from the beginning to the end. First, anonymous access to the Internet poses the most serious threat. In many countries, one of the most important forms of using the Internet is realized through cyber cafés or libraries, where anonymous users can access many of the online services. Definitely, there exist different situations in different countries. Compared with Finland where there are few cyber cafés in towns and cities, the cyber cafés in China have become the "third space" of school-aged juveniles besides home and school. The facilities and services in academic or public libraries are far less convenient for users than those in cyber cafés managed by private firms. An increasing number of hacking cases involving the Internet or Internet users are committed or conspired in cyber cafés.

Secondly, anonymous subscription to the Internet services raises the difficulty of identifying users. The personal information provided for the registration of an e-mail

account, the name and address of e-mail messages, and the authors' information in Usenet, etc., can all be fabricated. Keeping identity anonymous is favourable for the protection of users from victimization, but it also favours the hiding of perpetrators from being traced.

Thirdly, users can keep their identity anonymous in the process of online communications. There are also mechanisms for keeping complete anonymity by which one user can send messages to other users, and then the messages are transmitted to the final target, such as newsgroup, e-mail list, or a single e-mail account. What makes it more complex is that in the mechanisms the intermediary can only be a programme and may be in another jurisdiction (Kingdon 1994). This also reminds us that there exists the possibility of numerous transmitting points, by which messages are transmitted from one terminal to the next terminal, from that to the next in line, and so on, until the message reached the destination.

Tracing this transmitting process is theoretically possible. During the tracing process, the investigation is exactly the contrary to the process of transmission. Each time, the investigator can trace back one point.

It is likely that all points are identifiable. Nevertheless, as long as there is an unexpected element at any point, the tracing chain can be disrupted without reaching the original source. According to National Police Agency of Japan (1998), the possible examples include that the victim has no record of the Internet Protocol (IP) address; ISPs do not keep suitable records; hackers alter the logs; or some points are located in countries that have not criminalized hacking. As Koch (Inter*@ctive Week*, 10 July 2000) has pointed out, theories about detection remain theories, and they are too new to be tested in practice. Even if all the work of traceback is fulfilled, the actual value of this work may be discounted in a judicial process because of different locations and thus diversified jurisdictions.

Fourthly, the specific service or software can play further roles in hiding users. Cybercriminals usually establish anonymizers, which are systems particularly designed to invalidate technical identification of the source of communications (See Belgium's answer to the "Questionnaire 5: Have you received any reports from your law-enforcement authorities that have indicated an obstruction of their work due to the non-

existence of appropriate legal instruments concerning traffic data retention?" in Council of the European Union, Council doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1, Brussels, 20 November 2002). In fact, this kind of service or software can also be conveniently obtained free of charge or at an inexpensive price from the Internet. Everyone who is online can get access to these tools and services. Such software is likely to be replicated and spread unlimitedly, creating a bigger population of hidden users who potentially threaten the security of information systems.

Although the anonymity of cybercriminals poses a series of questions, it is still the core of the "perfect environment" for the criminals. Levinson (2002, p. 455) said that anonymity is exploited by perpetrators of old crimes such as fraud, pornography, gambling, stalking and identity theft, or new crimes such as unauthorized access, denial of service, and malicious programmes. Yet it is at the same time welcomed by Internet users. People are constantly concerned that without online anonymity, it could be impossible to guarantee fundamental rights (COM(2000) 890 final, p. 20; National Police Agency of Japan 1998). It is not strange that the European Union Data Protection Working Party's Recommendation recognized that online anonymity brings about a dilemma for governments and international organizations (The Article 29 Data Protection Working Party 2001): in particular, in maintaining human rights to privacy and freedom of expression, and combating cybercrimes (COM(2000) 890 final, p. 20). Philip (2002) warned that anonymity can provide users with "the courage to do the outrageous and sometimes even resort to illegal activities."

Mitchell and Banker (1997, pp. 707-711) have concluded that there are four characteristics in which cybercrimes are different from traditional crimes, that is to say, difficulties in detection, limited reporting, jurisdictional complexities, and resource constraint. All these four aspects fall under the broad characteristic of concealment. The concealment of cybercrimes has been brought about by other technological and human factors (Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006).

Most of traditional offences are greatly observable due to apparent depredations, presence of witnesses, and so on. There are also traditional crimes that occur in private places and become less visible (Walsh 1983, p. 236). Unlike traditional threats where

criminals are physically present at the crime scene, cybercriminals are usually not present at the crime scene thus making apprehension difficult (Speer 2000, p. 260). In information systems, executing a command to delete files does not mean that the files are permanently deleted. What happens is merely that files are hidden due to a change in file names so that the files can be recovered. In United States v. Angevine (Tenth Circuit No. 01-6097, D. C. No. 00-CR-106-M, 22 February 2002), "the computer expert used special technology to retrieve the data that had remained latent in the computer's memory," though the accused had attempted to delete the relevant files. In United States v. Upham (First Circuit No. 98-1121, 12 February 1999), the investigator used the "undelete" function of a programme to recover deleted files from the deposit media, as primary evidence in conviction. In Robertson v. Her Majesty's Advocate ([2004] ScotHC 11 (17 February 2004)), the police recovered 347 deleted images from the unallocated space, and 878 images and 45 movies from deleted zip file within the disc. Only when a secure-eraser programme is in use, the files are permanently deleted. For example, in the case of International Airport Centres, L. L. C., et al v. Jacob Citrin (Seventh Circuit No. 05-1522, 24 October 2005) (p. 2). Skilful criminals can disable this kind of security mechanism, and conceal the data that might possible be taken as evidence in prosecution. Technological advances have both a positive impact on businesses and a negative impact on law enforcement (Institute for Security Technology Studies 2002). For example, in the DrinkOrDie case, the online software piracy group concealed its actions by various security measures: exchanging e-mails via private mail server using encryption; using a nickname to identify members, and communicating about group business only in closed, invite-only IRC channels; the FTP sites, where tens of thousands of pirated software, game, movie, and music titles were deposited, were secured by particular authentication mechanisms (U. S. Department of Justice, Press release, 17 May 2002). On the other hand, the available technological solutions have not completely met the requirement of data collection, log analysis, and Internet protocol tracing (American Society for Industrial Security 2004, p. 40). There is also the necessity for law-enforcement agencies to recruit personnel with "electrical engineering and computer-science backgrounds" (Fields 2004, p. B1);

Inevitably, critics point out that cyber police have extra incentives than combating

cybercrime, for example, asking for more money, more wiretap, bugs in computers and sell phones, weak encryption and permission to implement security technology, without more arrest following (Koch Inter@ctive Week, 10 July 2000).

Concealment of crimes has important economic effects. Stanley (1995, p. 2) stated that concealment of crime can decrease the incentives not to perpetrate, and increase the costs of law enforcement. Concealment of cybercrime demonstrates the low probability of punishment. In the U. S., only one in 100 cases was detected, one in 8 prosecuted, while only one in 33 prosecuted cybercrimes resulted in a prison sentence. That is to say, the likelihood that a cybercriminal would be put into prison was a one in 26,400 chance (Daler and co-workers 1989, p. 22), as compared with the likelihood of imprisonment in traditional bank robbery a one in three chance (ibid.). Law-enforcement agencies found that a majority of cybercrimes never reached the criminal-justice system. Even in the relatively few cases where a crime was reported, most often the criminal's identity was never discovered. As a consequence, as Radzinowicz and King (1977, p. 67) pointed out, "The calculation of chance is as applicable to the commission of crime as to many other activities." Given other factors constant, if cybercrime is more concealed than other offences, the potential perpetrators are more motivated to take illegal actions on the Internet, and thus more offenders of traditional crime will be prepared to migrate to cyberspace.

TRANS-TERRITORIAL ANONYMITY

Free flow of information from one state to another is a purpose of information systems (Directive 95/46/EC, Preamble (3); UN A/RES/51/162; Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 12), but trans-border flow is not free (The Convention mentioned above, Article 12 provides the limit on trans-border transfer of data). The trans-border information flux is accompanied by risks of crime of a similar nature. In any country, the court must have jurisdiction over the person or the subject-matter of a lawsuit. This works well with the current set-up of law-enforcement agencies that are territorial and are operating in different villages, towns, districts, cities, counties, states or provinces, or national

boundaries. Nevertheless, unauthorized access to information systems can be accomplished from virtually anywhere on the networks (See cases such as United States v. Tenebaum (Israel), 18 March, 1998, involving an Israeli hacking United States military computers; United States v. Gorshkov (W.D. Wash) 4 October 2002, Russian hacker; United States v. McKinnon I (E.D. Va.) and II (D. N.J.) 12 November 2002, British National Hacked into the U. S. Military Networks; United States v. Zezev (S.D. N.Y.) 1 July 2003, Hackers from Kazakhstan; United States v. Ivanov (D. Conn.) 25 July 2003, Russian hacker), because the communications capability of cyberspace allows criminals to conspire more easily, without geographical proximity to one another or to the target (Lenk 1997, pp. 126-135). The international characteristic of cybercrime is evident (National Police Agency 1998). In fact, some of the cases prosecuted have been of this nature, for instance, R. v. Kozun (2007 MBPC 7), where the forensic analysis of the computer of the accused disclosed that 165 separate users from 15 countries had traded through his computer. The computer was converted into an automated trading centre through a programme, by which 141 users had traded in the previous 13 days.

The sphere of legal jurisdiction makes the cybercrime enforcement more complicated (Lee and co-workers 1999, p. 873). Smith, Grabosky, and Urbas (2004) concluded that the trans-national dimension of cybercrime posed four formidable challenges for prosecutors, who have to determine whether the conduct in question is criminal in their own jurisdiction, collect sufficient evidence to mobilize the law, identify the perpetrator, and determine his or her location, and decide whether to leave the matter to the local authorities or to extradite the offender (pp. 48-49).

Sinrod and Reilly (2000, p. 2) have pointed out that although some international organizations are examining cooperative mechanisms in the field of fighting against cybercrime, many of their members are slow in recognizing the urgency of the situation.

The elimination of borders favours inter-jurisdictional mobility of crime. Due to the actual difficulty in establishing jurisdiction, even if a certain offence is detected, it is still uncertain whether the way can easily lead to punishment. In R. v. Burns ([2003] NICC 13(2) (12 September 2003)), where the accused cloned mobile phones, or exploited faults or loopholes in the internal phone systems of companies or organizations to make cheap or free calls at the expense of those companies or organizations, the court found

that:

"As the investigation progressed it became more wide-ranging and involved another suspect and its ramifications were such that it eventually spread to other parts of the United Kingdom, to Tokyo, to South America, as well as to New Jersey and Atlanta in the United States of America. Several large organizations in the United Kingdom, other police forces and international telephone companies were involved. When it became apparent to the police that they did not have either the specialist equipment or the necessary expertise to access much of the information, specialist firms had to be engaged. All of this took a great deal of time." Reasonably, suggestions have been made to incorporate cyberspace into various jurisdictional frameworks. Nonetheless, this needs a great deal of time, agreement, and co-operation between countries, which are still struggling to take common actions.

Finally, it is worth noting that trans-national cases just make up a inconsequential part of cybercrime. No convinced conclusion can be drawn because it is probable that trans-national offences are not as prevalent as scholars have assumed. On the other hand, it is difficult to reveal these offences for reasons that scholars have laid bare. Or, it may be, that it is simply law enforcement does not put sufficient emphasis on these offences. Before credible data are available to give an answer to this question, we have certain reasons to claim that trans-national offences have sometimes of a dual nature: they do not appear as prevalent as domestic offences, but they are more difficult to detect and convict. In addition, because the investigation of trans-national offences is more expensive and time-consuming, law enforcement will not give more priorities to these offences than to cases that have happened "close to home".

Because information systems alone are no longer subject to the physical limit of traditional countries, we can expect that many offences traditionally committed in neighborhoods, communities, and native areas now extend beyond national boundaries. Many other offences traditionally committed in a trans-border manner are becoming a means to acquire new markets in the more networked globe. Some new offences can, indeed, only be completed in a trans-national style. Trans-national crime can be seen as the counterpart of international trade in civil society, being an involuntary transaction

between perpetrators and the social order (in many cases, involving victims, but in many other cases, victimless).

For example, in McKinnon v USA & Anor ([2007] EWHC 762 (Admin) (03 April 2007)), the accused used his own computer in London and obtained unauthorized access to dozens of governmental computers of the U. S., from which he discovered the identities of certain administrative accounts and associated passwords. He installed remote control software on these administrative computers. The software enabled him to access and change data at any time.

Many people have taken it for granted that because computer networks are trans-national, naturally most crimes committed in relation to the networks are also trans-national. This poses a great concern among academia, law-enforcement agency, and legislature. However, this is still an unanswered question: firstly, information systems have crossed the national boundaries, but prosecuted offences are mostly confined within these boundaries; secondly, due to lack of an international arrangement of law and enforcement, few trans-national cybercrime offenders have been investigated; and thirdly, offences are mostly territory-dependent, and do not cross the border at all.

All these factors are responsible for the low likelihood of trans-national cybercrime, but, as we have seen and will see further, the absence of international legal harmonization and assistance mechanisms contributes primarily to the current invisibility of trans-national cybercrime.

IMPACT OF CYBER ANONYMITY ON CRIMINAL MOTIVATION AND VICTIMIZATION

Lack of punishment reduced the expected cost of the criminals, which were composed thus of moral costs and substantial costs, specifically, the perpetrators' necessary devices and labour in cybercrime. Because there was no cybercrime law, there was neither expected punishment nor the expected cost induced by the expected punishment. Under such circumstances, the probability of conviction equalled zero. The expected utility of the perpetrator almost equalled the utility of a situation in which crime went undetected or unpunished. According to an economic analysis of crime (Becker 1968, pp. 169-217),

those who are risk-indifferent are indifferent to detection and conviction. For those who are risk-lovers, cybercrime becomes a new cause, a new chance, a new challenge, and a new type of risk. For those who are risk avoiders, because of the low risk of detection and conviction rate of cybercrime, they transfer from other offences to cybercrime. Therefore, the number of cybercrimes and perpetrators will inevitably increase.

The low cost of cybercrime and the difficulty in detection and evidence collection create incentives for potential perpetrators. The nature of high intelligence, trans-territoriality, and high concealment of cyber transgress and cybercrime make it difficult to detect and investigate the cases (See Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006). Stating from another standpoint, cybercrime surpasses the current capacity of public and private regulators to control (Grabosky 2000, p. 2). As for the transgressors or criminals, they usually only need to click the mouse or knock the keyboard at home or in the office in order to commit the illegality in a short time. The risks and costs are in cybercrime lower than those in traditional crime, while the benefits are higher. This cost-effectiveness further strengthens the mind of the perpetrator to commit cybercrime.

Cybercriminals have a greater advantage than most of the traditional criminals in respect of the low probability of arrest and conviction. Hatcher and co-workers (1997, pp. 397, 399.) have pointed out that many cybercrimes are not reported. The term “dark figure”, used by criminologists to refer to unreported or unrecorded crime, has been applied to denote undiscovered cybercrimes (UNCJIN 1999, Paragraph 30). As Radzinowicz and King (1977) pointed out that, “The recorded figures of crime are huge but the reality behind them everywhere looms far larger. The sinister word dunkelziffer (dark figure) was coined at the turn of the century to express this hidden reality.” (p. 42). Many intrusions are not detected for a variety of reasons (COM (2000) 890 final, p. 11). Cybercrimes can well be described as hidden crimes, which is used by Cook (1997) to denote under-reported or under-recorded crimes such as domestic violence, sexual assault, and racial harassment (p. 55-58), the counterpart of which is “hidden victims,” denoting the victims of the “hidden crimes” (p. 127).

At the same time, victims of cybercrime are keen to be hidden victims (Cook 1997, p. 127). The usual “motives for silence” pertaining to victimization may fall into one of the

following categories: 1. The idea that the victimization is not worth the mobilization of justice; 2. Involvement; 3. Pressures of fear; 4. The perturbed accessibility of police and court; and 5. The ignorance of events by the police (Radzinowicz and King 1977, pp. 38-40).

In sketching the victim decision-making, Greenberg and Ruback (1985) have established a three-stage model: the victim judges whether the event is a crime, evaluates its seriousness and decides what to do (Greenberg and Ruback 1985, as cited by Feldman 1993, p. 26). Before these stages, one stage that is more essential should be included, that is, whether the victim knows the event. If this is the case, the reporting of cybercrime might stay at a lower level, because cybercrime is imperceptible and thorny to notice; it is much trickier for the victim to judge whether the event is a crime and to estimate the losses; and the victim has less awareness of whether there is an agency to report the crime. The limited reporting of the cybercrime has been noted more than 20 years ago by Parker and Nycum (1984, p. 313), who studied the invisibility of computer crime. At present, the Internet's virtual environment has made the circumstances still poorer. Auspicious progress in proving material evidences in traditional crimes was made in late 1980s when DNA tests were first introduced (Levinson 2002, p. 537). Nonetheless, digital evidence in computer crime is untouched by such high-technological testing measures. The invisibility of cybercrimes is based on numerous factors, either technical or artificial (UNCJIN 1999, Paragraphs 30, 31). Sometimes, the straightforward cause is that the victims are not enthusiastic to report, or even do not know where to report the case (Salgado 2001). The acknowledged reasons for the reluctance to launch legal actions are principally fear of undesirable publicity, public humiliation or loss of goodwill, loss of investor or public confidence, resulting economic consequences such as the panic effect that this information would create on their stock prices (See Carter 1995, p. 21; Roush 1995, pp. 32, 34; Gelbstein and Kamal 2002, p. 2; McKenna 2003), and exposure to future attacks (COM (2000) 890 final, p. 11). The UN suggested that these factors have a momentous impact on the detection of cybercrime (UNCJIN 1999, Paragraph 31).

Yet there are other reasons for the victim to remain silence. While many people are vigorous in maintaining their interests and rights, some people view victimization as

their own malfunction in life and profession and are not enthusiastic to expose the reality of their failure to any individuals and institutions, so as not to make public their own disadvantage.

Therefore, it is unavoidable that the rate of unidentified instances of cybercrimes has increased as a consequence. The 2013 Australian Cyber Crime and Security Survey Report summarized the reasons why respondents did not report cyber security incidents, 44% of them said "there are no benefits of reporting"; 44% chose "other", meaning that the incidents and the consequences were minor, and that the incidents were reported internally and managed by corporate policy; 20% said that "the attackers probably wouldn't get caught &/or prosecuted"; 16% of them "did not know"; and 12% worried about "negative publicity for the organisation" (CERT Australia 2014, p. 35). This and other similar surveys has indicated the percentages of respondents identifying each stated rationale as being very imperative in their assessment not to report computer intrusion. At the same time, it is worth noting that the reasons are subject to changes in each yearly study.

CONCLUSION

Without ignoring all its merits, cyber anonymity has deep impact on occurrence of cybercrime, mostly reducing the potential likelihood of detection and thus its costs. In fact, anonymity may to some extent encourage potential perpetrators to take the risk. On the other hand, victims may lose opportunities to make judgment on whether or not it is of their interest to interact with hidden perpetrators. Once crime occurs, anonymity further hinders law enforcement from detecting and investigating.

In recent year, wrestling between claims for and against cyber anonymity has been continuing. However, there has some new advancement in judicial sector. The European Union Court of Justice issued a decision on May 13 2014, in case C-131/12 (Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez), ruling that the "right to be forgotten" is embedded in the provisions of Directive 95/46/EEC (Iglezakis 2014, p. 4). The right to be forgotten is a special field of cyber anonymity. If cyber anonymity is not imposed any limit, vulnerable users and

incompetent law enforcement cannot cope with problems accompanying it. Therefore, the right to be forgotten applies only where the information is "inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing" (para 93 of the ruling). the Court unambiguously spelt out that the right to be forgotten is not unconditional but will always have to be "balanced against other fundamental rights", for instance the freedom of expression and of the media (para 85 of the ruling). Absolute freedom of anonymity should not be allowed as the case in the real society. There is a necessity to balance the needs to protect privacy and prevent cybercrime (Shinder, 2011).

REFERENCES

1. American Society for Industrial Security (ASIS). 2004. Cybercrime-Fighting Tools Still Lacking, *Security Management*, no. 40.
2. Becker, G. S. 1968. Crime and Punishment: An Economic Approach, *Journal of Political Economy*, vol. 76, pp. 169-217.
3. Carter, D. L. 1995. Computer Crime Categories, *Law Enforcement Bulletin*, U. S. Department of Justice: Federal Bureau of Investigation, vol. 64, no. 7, pp. 21-26.
4. CERT Australia. 2014. The 2013 Australia Cyber Crime and Security Survey Report. Commonwealth of Australia.
5. Clark, F. and Diliberto, K. 1996. *Investigating Computer Crime*, Boca Raton, Florida: CRC Press LLC, 1996.
6. Commission of the European Communities. 2000. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime*, COM (2000) 890 final.
7. Conly, C. H. 1991. *Organizing for Computer Crime Investigation and Prosecution*, Darby, PA: Diane Publishing.
8. Cook, Dee. 1997. *Poverty, Crime and Punishment*, London: CPAG.
9. Daler, T., Gulbrandsen, R., Melgrd, B. and Sjølstad, T. 1989. *Security of Information and Data*, Chichester: Ellis Horwood.
10. Debose, B. 2004. Kerry Says Threat of Terrorism Is Exaggerated, *The Washington Times*, 29 January.

11. Dodge, M. and Kitchin, R. 2001. *Mapping Cyberspace*, New York, New York: Routledge.
12. Edwards, L. and Walde, C. (eds.). 1997. *Law and the Internet - Regulating Cyberspace*, Oxford: Hart Publishing.
13. Ekman, P. 1992. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*, New York: Norton.
14. European Commission. 2014. Factsheet on the right to be forgotten ruling C - 131/12. Retrieved 5 Feb. 2015, from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
15. Fields, G. 2004. Cyberexperts and Engineers Wanted by FBI, *Wall Street Journal*, B1, 6 April.
16. Gelbstein, E., and Kamal, A. 2002. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research.
17. Grabosky, P. 2000. Cyber Crime and Information Warfare, in Proceedings of the Transnational Crime Conference, Canberra, 9-10 March. Retrieved 5 Feb. 2015, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf
18. Greenberg, M. S. and Ruback, R. B. 1985. A Model of Crime Victim Decision Making, *Victimology: An International Journal*, vol. 10, pp. 600-616.
19. Hatcher, M. and co-workers. 1999. Computer Crimes, *American Criminal Law Review*, vol. 36.
20. Howitt, D. 2002. *Forensic and Criminal Psychology*, Essex, England: Pearson.
21. Hunt, Allan. 1993. *Explorations in Law and Society: Towards a Constitutive Theory of Law*. New York, London: Routledge.
22. Iglezakis, I. 2014. The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet? Retrieved 5 Feb. 2015, from http://dx.doi.org/10.2139/ssrn.2472323
23. Institute for Security Technology Studies (ISTS). 2002. *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment*.

24. Internet Crime Forum IRC Subgroup. 2001. *Chat Wise, Street Wise-Children and Internet Chat Services*.
25. Internet World Stats. 2014. World Internet Usage and Population Statistics – June 30, 2014 Mid-Year Update. Retrieved 5 Feb. 2015, from http://www.internetworldstats.com/stats.htm
26. Johnson, T. A. 2006. *Forensic Computer Crime Investigation*, Boca Raton, Florida: Taylor and Francis Group.
27. Khosrow-Pour, M. 1998. *Effective Utilization and Management of Emerging Information Technologies*, Hershey: Idea Group Publishing.
28. Kingdon, J. 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 5 Feb. 2015, from http://www.catalaw.com/logic/docs/jk-isps.htm
29. Koch, L. Z. 2000. Open Sources Preventing Cybercrime, *Inter@ctive Week*.
30. Lee, M. and co-workers. 1999. Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, *Berkeley Technological Law Journal*, vol. 14, no. 2, pp. 839-885.
31. Lenk, K. 1997. *The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing, The Governance of Cyberspace*, New York: Routledge, pp. 126-135.
32. Levinson, D. (ed.). 2002. *Encyclopaedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.
33. Li, X. 2008. *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*, Turku: Uniprint.
34. Mandia, K. and Prosise, C. 2003. *Incident Response and Computer Forensics*, Emeryville, California: McGraw-Hill/Osborne.
35. McKenna, B. 2003. United Kingdom Police Promise Charter to Guard Good Names, *Computers and Security*, vol. 22, no. 1, pp. 38-40.
36. Mitchell, S. D., and Banker, E. A. 1998. Private Intrusion Response, *Harvard Journal of Law and Technology*, vol. 11, no. 3, pp. 699-732.
37. Mohay, G., Byron, C., Vel, O., McKemmish R., and Anderson, A. 2003. *Computer and Intrusion Forensics*, Norwood, Massachusetts: Artech House.

38. NPA. 1998. *The Situation of High-tech Crime and the Suppression of Police, Japan Police White Paper*, Tokyo: National Police Agency.
39. O'Brien, T. 2004. Risk and Conflict Challenges for New Zealand, *Auckland War Memorial Museum Symposium Push for Peace*.
40. OECD. 2004. *Second Organization for Economic Cooperation and Development Workshop on Spam: Report of the Workshop*, JT00174847, Busan, Korea.
41. OECD. 2005. Task Force on Spam, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, Paris, France.
42. Parker, D. B., and Nycum, S. H. 1984. Computer Crime, *Communication of the ACM*, vol. 27, no. 4, pp. 313-315.
43. Philip, A. R. *The Legal System and Ethics in Information Security*, SANS Institute, 2002. Retrieved 5 Feb. 2015, from http://www.securitydocs.com/go/1604
44. Radzinowicz, L. and King, J. 1977. *The Growth of Crime: The International Experience,* London: Hamish Hamilton.
45. Robertson, S. 2000. The Digital City's Public Library: Support for Community Building and Knowledge Sharing, in Toru Ishida and Katherine Isbister (eds.) *Digital Cities: technologies, Experiences, and Future Perspectives*, Springer, pp. 246-260.
46. Roush, W. 1995. Hackers: Taking a Bite Out of Computer Crime, *Technology Review*.
47. Rowland, D. 1998. Cyberspace - A Contemporary Utopia? *The Journal of Information, Law and Technology*, vol. 1998, no. 3. Retrieved 5 Feb. 2015, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/rowland/
48. Salgado, R. P. 2001. Working with Victims of Computer Network Hacks, *USA Bulletin*, vol. 49, no. 2.
49. Shinder, D, 2011. Online Anonymity: Balancing the Needs to Protect Privacy and Prevent Cybercrime. Retrieved 5 Feb. 2015, from http://www.techrepublic.com/blog/it-security/online-anonymity-balancing-the-needs-to-protect-privacy-and-prevent-cybercrime/

50. Sinrod, E. J., and Reilly, W. P. 2000. Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, *Computer and High Technology Law Journal*, vol. 16, pp. 177-232.
51. Smith, R. G., Grabosky, P. and Urbas, G. 2004. *Cyber Criminals on Trial*, Cambridge: The Press Syndicate of the University of Cambridge.
52. Speer, D. L. 2000. Redefining Borders: The Challenges of Cybercrime, *Crime, Law and Social Change*, vol. 34, pp. 259-273.
53. Stanley, T. J. 1995. Optimal Penalties for Concealment of Crime, *Economics Working Paper Archive*.
54. Stephenson, P. 2000. *Investigating Computer-Related Crime*, Boca Raton: Florida: CRC Press LLC.
55. The Article 29 Data Protection Working Party. 2001. Fourth Annual Report on the Situation Regarding the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in the Community and in the Third Countries Covering the Year 1999.
56. UNCJIN. 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, *International Review of Criminal Policy*, nos. 43 and 44.
57. Vacca, J. R. 2005. *Computer Forensic: Computer Crime Scene Investigation*, Hingham, Massachusetts: Charles River Media.
58. Walsh, D. P. 1983. Visibility, in Dermot Walsh and Adrian Poole (eds), *A Dictionary of Criminology*, London, Boston, Melbourne and Henley: Routledge and Kegan Paul.
59. Weimann, G. 2004. Cyberterrorism: How Real is the Threat? *United States Institute of Peace Special Report*, no. 119.
60. Wilbur. S. 1997. An Archaeology of Cyberspace: Virtuality, Community, Identity, in D. Porter, (ed.), *Internet Culture*, London: Routledge, pp. 5-22.
61. Yi, M. 2006. Associated with Traditional Crime, Cybercrime Threats Citizens Safety, *Huanghai Morning Newspaper*, 27 January.
62. Zigrus, I. 2001. Our Virtual World: The Transformation of Work, Play, and Life via Technology, IGI Global.