COLLABORATIVE POLICING AGAINST ONLINE IDENTITY THEFT : A STRATEGIC PROPOSAL OF THAILAND FOR LAW ENFORCEMENT*

กิจการตำรวจแบบร่วมมือเพื่อต่อต้านการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ : ข้อเสนอเชิงยุทธศาสตร์ของประเทศไทยสำหรับหน่วยงานบังคับใช้กฎหมาย

Chitphol Kanchanakit, Ph.D.**

Abstract

Referring to the resolution to the problem of cybercrime adopted at the 29 ASEANAPOL Conference in 2009, this article aims to present the approach of collaborative policing against online identity theft gained from the stakeholders analysis. The article is divided into five parts beginning with the characteristics of online identity theft and the situation in Thailand. The second part provides the concept of partnerships applied to prevent crime. The third part places an emphasis on partnerships in online policing against identity crime. The fourth part evaluates the actions of Thailand against online identity crime. In the final part, possible recommendations are proposed to protect personal information in cyberspace from identity fraudsters. Since the roles of law enforcement agencies in ASEAN countries are not sufficient to fight online identity theft due to the difference of each state's law and policy and abundant networks of online society all over the world, The ASEAN states should implement a concept of strategic partnership by seeking more collaboration and cooperation with concerned private and public partners.

Keywords : Online identity theft, Collaborative policing, Strategic partnership

*This article is a part of the research paper submitted for fulfillment of Regional Executive Leadership Program done by Jakarta Centre for Law Enforcement Cooperation- JCLEC, Indonesia in 2013

**Lecturer in law at Southeast Bangkok College, Thailand, e-mail : interpolck@yahoo.com

บทคัดย่อ

อ้างถึงข้อมติในการจัดการปัญหาอาชญากรรมคอมพิวเตอร์ซึ่งได้ยอมรับในที่ประชุมหัวหน้าตำรวจอาเซียนครั้งที่ 29 เมื่อปี 2009 บทความนี้มีวัตถุประสงค์เพื่อนำเสนอกิจการตำรวจแบบร่วมมือเพื่อต่อต้านการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์โดยใช้การวิเคราะห์ความเป็นหุ้นส่วน บทความนี้แบ่งออกเป็น 5 ส่วน เริ่มต้นจากการพรรณนาถึงลักษณะของการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์และสถานการณ์ในประเทศไทย ส่วนที่สองได้อธิบายถึงแนวคิดการเป็นหุ้นส่วนในการป้องกันอาชญากรรม ส่วนที่สามมุ่งเน้นไปที่หุ้นส่วนในด้านการตรวจตราทางคอมพิวเตอร์เพื่อต่อต้านอาชญากรรมการโจรกรรมข้อมูลส่วนบุคคล ส่วนที่สี่เป็นการประเมินการดำเนินการของประเทศไทยต่อการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ และส่วนสุดท้ายได้ให้ข้อเสนอแนะในการคุ้มครองข้อมูลส่วนบุคคลบนคอมพิวเตอร์จากการถูกโจรกรรมโดยมิจฉาชีพ เนื่องจากหน่วยงานบังคับใช้กฎหมายในประเทศอาเซียนไม่ได้แสดงบทบาทอย่างเพียงพอในการต่อสู้กับการโจรกรรมข้อมูลส่วนบุคคลอันเนื่องจากความแตกต่างทางกฎหมายและนโยบายของแต่ละประเทศ และเครือข่ายทางสังคมทางคอมพิวเตอร์จำนวนมหาศาลของทั้งโลก รัฐอาเซียนจึงควรนำแนวคิดหุ้นส่วนเชิงยุทธศาสตร์ไปใช้ในทางปฏิบัติโดยแสวงหาความร่วมมือกับหุ้นส่วนภาคเอกชนและภาคประชาชนที่เกี่ยวข้อง

คำสำคัญ : การโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ กิจการตำรวจแบบร่วมมือ ความเป็นหุ้นส่วนเชิงยุทธศาสตร์

Introduction

Online identity theft is a novelty of cybercrime that adversely affects citizens in cyberspace. The increasing use of personal information to make important decisions and the widespread transfer of information between a variety of public and private organizations facilitate theft of identity than traditional ways of privacy violation (Solove, 1997). Not with standing internet users' awareness of information security, the computer technology makes it easier for criminals to reach individual data in computer system and steal it for personal pecuniary gain. Accordingly, law and criminal policy should be developed to catch up with the advancement of identity crime and the strategy of public and private agencies should also be cooperatively modified to enable their employees to work together in creating safety nets for innocent users (Steinert, 1978). Nevertheless, due to the limited space, this article will only focus on the anti-cybercrime policy and management on online identity theft. Two main questions will be clarified. Firstly, are only states able to prevent and suppress online identity theft? Secondly, if not so doing, what should states do to improve their policy and strategies to deal with online identity crime?

Overview of identity theft

Identity theft is a crime in which the stealing personal information such as name, date of birth, address and social security number from individual, public and private records unlawfully and then transferred or sold to perpetrators to commit a range of further offences including various types of fraud (Jewkes, 2010). Personal data can be stolen by various ways; for example, pilfering mailboxes to obtain bank statements, dumpster diving and soliciting information through bogus job advertisement. Stolen identity is not only limited to be used for identity fraud, but also for further identity-related crime such as terrorism and drug trafficking (Gerard et al., 2004).

Identity thieves can access business databases by means of online surreptitious techniques through malicious software such as phishing, pharming and spyware to trick unsuspecting users to reveal private information (Wright, 2002). With stolen identities, the criminals can use it to commit the offences several times

around the world without appearing at the target location. The research on privacy and security concerns also found that the privacy and information security concerns are the major barriers for electronic commerce (Udo, 2001). It is estimated that the cost of identity theft to the British economy is around £ 2 billion annually.

In Thailand, stealing information can be committed through computer systems and internet without knowledge of its owner due to lack of a data protection law. Although the annual report of cyber criminal offences in accordance with the Computer-related Crime Act 2007 of Thailand shows cyber fraud is only ten per cent of crime committed online, it is uncertain whether how much online theft of identity is occurring due to underreporting. Thai research also found that the number of viruses and spyware sent via internet tends to increase every year whereas most of victims did not take any legal action against senders.

One of the possible ways to prevent identity theft is to take proactive actions to stop identity theft before it occurs. Law and policy thus could be the essential tools to impede online identity theft and strengthen collaboration among public and private agencies, whereas computer business firms may design digital code and technological device to prevent access to personal computer without permission (Lessig, 1999). Nevertheless, despite the difference of legal system in Asian countries including Thailand, integrated policy and cooperative networks between law enforcement agencies and their partners could be useful for impeding the proliferation of identity theft in cyberspace at this moment.

Concept of Anti-Crime Partnerships

Partnerships or coalitions represent a unique hybrid organism in the world of social interventions. Rosenbaum (2002) proposed the partnership model for crime prevention that is based on several key assumptions. To apply to prevention of cybercrime, the model postulates:

(1) Crime in cyberspace is complex and deeply rooted, requiring complex, innovative and comprehensive solutions

(2) Partnerships are better suited than individual agencies to identify and accurately define the target problems of greatest concern in a virtual

community. They are more likely to include diverse perspectives and theories about crime and violation of individual rights on computer system.

(3) Partnerships are better suited to developing created targeted interventions because they include a diverse group of individuals representing a diverse group of organizations with different philosophies of intervention.

(4) Multiple interventions are more effective than single interventions because each organization, especially public and private bodies can play the key roles in its specific areas.

(5) Appling similar reasoning, multiple agencies are more effective than single agencies. Representing different organizational cultures and services, partnership member bring more new ideas and resources to the problem-solving arena.

(6) As a corollary of 4 and 5 above, interventions that emanate from different domains–individual, family, peer group, netizens, computer business company, educational institutions and government–will maximize the total impact on the target audience. Multiple interventions by multiple agencies create the opportunity for the target group to be exposed to more than one intervention and thus experience cumulative effects.

(7) As a corollary of 4 and 5, exposure to different strategic mechanisms at different levels of intervention may yield new synergistic effects. That is, new effects can be created from the combinations of two or more interventions–interventions that produced no effects or different effects singularly.

If the above assumptions are valid, then partnerships can be expected not only to reduce crime online, but to serve a number of other functions as well. Partnerships, in theory, are expected to:

(1) Increase organizational accountability;

(2) Reduce fragmentation and duplication of services;

(3) Build public-private linkages;

(4) Increase public awareness of anti-crime initiatives;

(5) Strengthen local community organizations; and
(6) Permanently alter the way agencies "do business" by giving more attention to strategic planning, data-driven decision making, prevention, interagency cooperation, and public participation in virtual governance.

A theory of partnerships should go beyond group dynamics and group processes to delineate the various strategic intervention approaches employed by the group. The theory must pay special attention to the inter-organisational capacity to respond to problems with creativity, intensity, and/or coordination of interventions. The proposed model of partnerships suggests that interventions may have important characteristics that predict success–who will be doing what to whom with the support of what service agencies? Within this partnership framework, each agency brings a unique set of skills, experiences, resources, and intervention strategies to the table. The partnership provides a mechanism to exploit this capital by developing and implementing comprehensive and coordinated community-wide strategies at different levels (Rosenbaum, 2002).

Partnerships in online policing

Some commentators claim cyberspace is too broad to be governed by any single rule. However, Lessig (1999) argues that cyberspace can be technically managed by four constraints; digital code, law, market and social norms if they are designed and interacted appropriately. The actors involving cyberspace protection such as government, computer industry, civil society and public share their responsibilities to protect netizens from cyber threats. Likewise, as Wall comments, public police are only a small part of policing cyberspace and need the support of other public and private organisations in preventing cybercrime (Wall, 2010). The interdependence of public and private bodies thus makes them function coherently and share mutual advantages of all actors in the cyberspace in the form of a networked governance both in leadership and operational levels (Waarden, 1992). In this regard, understanding of the partnerships in cyber policing is useful to seek more collaboration for cybercrime prevention. The partnerships in cyberspace could generally be categorized into six main

groups; public police, non-governmental organisations, financial institutions, network infrastructure providers, media and internet user groups (Wall, 2007).

The first partnership is concerned with public police who normally are law enforcement units responsible for intelligence and investigation of cybercrime. In Thailand, Technology Crime Suppression Division (TCSD), the Royal Thai Police and the Division of Special Investigation (DSI) under the Ministry of Justice are two main law enforcement units responsible for taking preventive and countering measures against cybercrime. TCSD normally plays a primary role in investigating computer-related crime committed in Thailand and externally; however, in some cases involving transnational organised crime, the DSI's Committee may consider the level of seriousness of crime and impact on society and authorise the concerned unit of DSI to take over such a case.

The second partnership is private international organisations such as the US National Consumer Leagues' Fraud.org (NCL) representing consumers and workers on marketplace and workplace issues since its founding. NCL's Fraud.org provides necessary information to consumers by providing information of how to implement anti-virus software and filtering tools to protect computers from cybercriminals and government, businesses, and other organisations about the consumer's perspective on concerns including telemarketing fraud, identity fraud and identity theft. Unfortunately, Thailand has no policy to support the establishment of private organisations to investigate crime online.

The third partnership is banks and financial institutions which are the major actors involving the protection of personal data. Normally, a protection law requires the private company collecting and keeping personal information in their databases shall not disclose such information to third party without owner's permission. For example, the UK banks such as Barclays and Lloyds establish online security systems to protect money, personal information and customer privacy when cyber fraudsters are active. Fortunately, although e-banking in Thailand is popular, many banks and financial institutions have established many layers of security protection to boost consumers' trust while they are shopping online through VeriSign Trust.

The fourth partnership is network infrastructure organisations who provide Internet connection service for customers. Internet Service Providers (ISPs) are regarded as an intermediary to link the connection between users and Internet websites. ISPs can play a vital role in preventing cyberspace from potential criminals by regulating and filtering content online (Wall, 2002). In Thailand, although the Ministry of Information and Communication Technology (ICT) set out its strategic plans by calling for public-private agencies to work together to prevent cyberspace from the attack of cybercriminals, the cooperation between them is quite slow. The police always need to resort legal measures to request for searching and taking traffic data to investigate cyber suspects. This may be due to having no a central authority to command and control operation in practice.

The fifth partnership is media such as CNN, BCC and ABC, who can play an important role in raising public awareness of crime online by providing information of software and filtering tools to protect computers from cybercriminals. Similarly, Bangkok Post, the Thai newspaper, posted warning of digital identity theft on its websites and offering guidelines for customers and taking measures to protect computer systems from cyber attacks.

The last one is internet users and civil society who are the major users of cyberspace. Cyber-citizens can play a role by providing netiquette to regulate harmful activities in cyberspace (Council of Europe, 2009) and voluntary mechanisms of virtual policing (Wall, 2002). Not only does online community policing help promote safety content in cyber society, but it can also be used as an intermediary for reporting cybercrime between Internet users and public police. For example, Internet Hotline Providers in Europe (INHOPE) and CyberAngles are worldwide networks of Internet users providing online safety information and collaborating with law enforcement to fight the trading of online pornography (Jewkes, 2010). Nevertheless, the enforcement of social norms in cyberspace in Thailand seems to be ignored by public and private organisations.

Assessment of Thailand's actions against online ID theft

Even though online identity theft is rather new in terms of crime prevention in Thailand, the law enforcement agencies have seriously attempted to seek more preventive measures to protect internet users from this cybercrime. For example, TCSD, the Royal Thai Police made several campaigns to raise public awareness of crime online via media. In this sense, assessing Thailand's capacity to fight identity crime is useful for finding out the possible solutions by considering the strengths, weaknesses, opportunities and threats of orgnisations, the so-called "SWOT analysis."

Firstly, Thailand has taken progressive action by setting up policy and operational agencies to deal with cybercrime. The Ministry of Information and Communication Technology (ICT) plays an important role in administering the public agencies under its control and issuing the ministerial rules for the purpose of the execution of the Computer-related Crime Act 2007. For example, ICT issued its strategic plan in 2007 calling for public-private agencies to work together to prevent information system from destruction caused by various means including cybercrime and terrorism (ICT, 2007). Additionally, TCSD is a professional unit working with other government and non-government agencies both in national and international levels in investigating cybercrime according to the cybercrime law.

Secondly, Thailand has adopted a multi-directional policy to align with many developed countries such as the United States of America, Australia, Japan and Singapore, which can potentially provide financial and technical support to fight cybercrime. For example, USA has supported the establishment of International Law Enforcement Academy (ILEA, Bangkok) providing training programs on cybercrime investigation for more than 10 years. International training courses equip officers with modern skills to investigate technically criminals across borders. Transnational Crime Coordinating Centre supported by Australian Federal Police is also a key mechanism working closely with Royal Thai Police in collecting and analyzing data on transnational crime networks through Case Management of Intelligence System (CMIS), which could help police investigation in the Asia-Pacific region.

Thirdly, unfortunately, although Thailand amended its Penal Code and established the Cybercrime Act in 2007 to cover various types of crimes online, the

laws are still silent on the issue of stealing personal information. Theft of personal information has never been criminalized and the data protection law has not been endorsed by the Parliament. Additionally, due to the complexity of digital technology and cyberspace, learning about cybercrime among law enforcers is quite slow, whereas public-private collaboration seems to be ineffectively implemented in line with the ICT strategic plan.

Fourthly, cyber and physical criminals have potential to exploit the advancement of technological communication and create criminal networks to commit crime across countries by developing new ways to hide online police and lure victims into their traps. Innovative cybercrimes can be continuously seen through new technological forms of identity theft such as sending spyware to target computer and voice over internet protocol (CIPPIC, 2007). As a result, it is time for the government to set up specific policy for public-private cooperation to safeguard internet users.

In summary, Thailand has not had the effective laws to protect information stored in databases both offline and online, the public-private cooperation on cybercrime prevention is quite slow, especially in terms of sharing information and responsibility. As a result, the Royal Thai Police, as a key actor of policing cyberspace, should take proactive action by reminding public and private partners to understand the nature of cybercrime and adjust their policy to cope with online identity theft. In practical, Chiefs of Police should play the roles by mobilizing leadership at all levels of public and private organizations to realise the problems of online identity theft and work together to protect this crime. A Plan of Action for collaborative policing could also be set up in line with public-private cyber security policy to assure that each partner would engage in cyberspace appropriately.

Recommendations for Law Enforcement Agencies

As mentioned previously, although the ASEAN Chiefs of Police Conference called for more cooperation on information sharing, cybercrime investigation and mutual assistance in criminal matters, it seemingly overlooks the role of private stakeholders. They could potentially assist the police by reporting cybercrime,

providing computer experts to set up digital code, raising public awareness through various campaigns and securely storing customers' information. The challenge for police leaders is how to build up mutual trust and more collaboration between public and private bodies in securing cyberspace. This paper proposes the Royal Thai Police and other ASEAN police forces should address the increase in cybercrime and adjust their policy and strategies to tackle online identity theft in a multi-layered approach as follows;

- to strengthen collaboration with Internet Service Providers and computer firms to take proactive action in investigation of cybercrime such as locating the sites of offenders, filtering illegal contents and blocking illegal websites on their servers.

- to collaborate with media and non-governmental organisations to set up social norms for cyberspace and lead public awareness campaigns on cybercrime to protect internet users from various types of identity theft.

- to seek more cooperation with academic institutions such as computer forensics and criminal justice courses in universities, the software industry should develop computer software to counter cybercrime. This may include setting up training programs and workshops in the gaining of knowledge and technical skills by law enforcement agencies.

- to encourage its ASEAN member countries and dialogue partners to work more closely with private organisations and civil society to secure cyberspace and identify cybercriminals in terms of information exchange, collaborative investigation training and raising public awareness. The ASEAN Chiefs of Police could be encouraged to adjust their policy and strategies to tackle identity theft.

Conclusion

The increase of online identity theft in Thailand and Asia has a negative impact on the law enforcement in cyberspace and the economic stability of countries. The complexity of the digital world and globalization inevitably makes law enforcement agencies work harder to bring offenders before justice. The government and law enforcers should thus pay more attention to the role of other public and

private partners including and civil society both in national and international levels in policing cyberspace. Collaborative policing could bring about mutual benefit for all stakeholders of cybercrime prevention by means of setting up social norms and technical barriers through cyberspace to protect personal information and raising public awareness of identity crime both online and offline. Chiefs of Thai Police can play more roles in policing cyberspace by calling for leadership in all levels of organizations on the basis of mutual trust. Furthermore, the Royal Thai Police should adjust its policy and strategies to seek more collaboration with its public and private partners in various activities such as the program of raising public awareness on online identity theft and joint task force against cybercrime so as to create online community policing and propose this approach to the next ASEANAPOL Conference for approval. If done so, the model could be used for the collective security in cyberspace and prevent identity crime in the region.

References

Canadian Internet Policy and Public Interest Clinic (CIPPIC). (2007). Australian, French and United Kingdom legislation relevant to identity theft : An annotated review. *CIPPIC working paper, March*(3C), 1-49.

Gerard, G. J., Hillison, W., & Pacini, C. (2004). Identity theft : The US legal environment and organisations related responsibilities. *Journal of Financial Crime,* (12), 33-43.

Jewkes, Y. (2010). Public policing and internet crime. In Jewkes, Yvonne & Yar, Majid (Eds), *Handbook of internet crime.* Devon: Willan Publishing.

Lessig, L. (1999). *Code and other law of cyberspace.* New York: Basic Books.

Rosenbaum, D. (2002). Evaluating multi-agency anti-crime partnerships: Theory, design, and measurement issues. *Crime Prevention Studies,* (14), 171-225.

Solove, Daniel J. (2003). Identity theft, privacy, and the architecture of vulnerability. *Hastings Law Journal,* (54), 1227-1235.

Steinert, Heinz. (1978). On the function of criminal law. *Contemporaries Crises*, (2), 167-193. Retrieved September 29, 2013, from http://www.springerlink.com/content/u8221758u26x200g/

Udo, G. J. (2001). Privacy and security concerns as a major barriers for e-commerce: A survey study. *Information Management and Computer Security, 9*(4), Retrieved October 1, 2013, from http://www.emerald-library.com/ft

Wall, D. (2002). *Insecurity and the policing of cyberspace*. New York: Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the Information age*. Cambridge: Polity Press.

Wall, D. (2009-2010). *Policing online behavior: How is cyberspace policed and by whom?, Cybercrime: Computer and crime in the information age.* Retrieved September 26, 2013, from http://webprod3.leeds.ac.uk/banner/dynmodules.asp?Y=201314&M=LAW-5336M

Warden, F. V. (1992). Dimensions and types of policy networks. *European Journal of Political Research,* (21), 29-52.

Wright, R. (2002). *Technology, and its effects on criminal responsibility, security and criminal justice*, International society for the reform of criminal law, 16th international conference. Retrieved October 5, 2013, from www.isrol,org/Papers/Wrihgt.pdfs.