Duty of Care Signatories in Digitally Signed Transactions and High Tech Theft
หน้าที่และความรับผิดของผู้ใช้ลายมือชื่ออิเล็กทรอนิกส์ในการลงลายมือชื่อในธุรกรรมอิเล็กทรอนิกส์

Pongthorn Somran
Assistant Professor at the School of Law
University of the Thai Chamber of Commerce
E-mail: psomran@hotmail.com

บทคัดย่อ

การใช้เทคโนโลยีไม่เพียงแต่ทำให้เกิดประโยชน์อย่างหลายประการ แต่ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงภัยและความรับผิดในการใช้เทคโนโลยีนั้นเช่นกัน ผู้ใช้เทคโนโลยีไม่เพียงแต่จะต้องพิจารณาถึงประโยชน์เท่านั้น จะต้องคำนึงถึงข้อเสียด้วย สาเหตุหนึ่งที่ทำให้การใช้ลายมือชื่อดิจิตทัลไม่มีประสิทธิภาพเนื่องจากการกระทำของเจ้าของลายมือชื่อ คู่กรณีที่เกี่ยวข้องกับลายมือชื่อดิจิทัล ผู้ออกใบรับรอง รวมถึงการกระทำของบุคคลภายนอกด้วย การกระทำของบุคคลภายนอก เช่น บุคคลที่แอบอ้างชื่อของบุคคลอื่น หรือผู้เจาะระบบ ถือได้ว่าเป็นการกระทำที่มีผลต่อการใช้ลายมือชื่อดิจิทัล การจารกรรมข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ อาจทำให้ผู้ใช้ลายมือชื่ออิเล็กทรอนิกส์ได้รับความเสียหาย การจารกรรมสามารถกระทำได้โดยการทำซ้ำกุญแจส่วนตัว ขโมยบัตรสมาร์ตการ์ดที่มีข้อมูลกุญแจส่วนบุคคลบันทึกไว้ หรือการที่เจาะเข้าไปยังฮาร์ดดิสก์ของผู้ใช้ลายมือชื่อดิจิทัล เนื่องจากการที่ลักษณะทางเทคนิคของการจารกรรมข้อมูลในโลกอินเทอร์เน็ต หรือการเจาะระบบข้อมูล การทำซ้ำกุญแจส่วนตัวหรือการเจาะระบบเข้าไปยังฮาร์ดดิสก์ของเจ้าของข้อมูลกุญแจส่วนตัวนั้นไม่สามารถเห็นได้ประจักษ์ชัดเช่นเดียวกับการจารกรรมหรือการบุกรุกโดยทั่วไป เจ้าของลายมือชื่อจึงไม่สามารถทราบได้ว่ากุญแจส่วนตัวของเขาถูกขโมยหรือถูกเจาะข้อมูลไป ในการวินิจฉัยความรับผิดของเจ้าของลายมือชื่อ จะต้องนำระดับความระมัดระวังของวิญญูชนมาพิจารณาด้วย เจ้าของ

ลายมือชื่อดิจิทัลจะต้องใช้ระดับความระมัดระวังตามสมควร อย่างเช่น วิญญูชนควรจะกระทำที่จะต้องดำเนินการเพื่อป้องการข้อมูลกุญแจส่วนตัวมิให้บุคคลใดเข้าถึงโดยไม่ได้รับอนุญาต ขโมย หรือให้บุคคลอื่นล่วงรู้ได้ ดังนั้นเจ้าของลายมือชื่อดิจิทัลจะต้องรู้ในสิ่งที่ชัดแจ้งที่เกิดขึ้นเช่นเดียวกันกับวิญญูชนที่รู้ถึงเหตุการณ์นั้นๆ อย่างไรก็ตาม การจารกรรมโดยวิธีไฮเทคนั้น ไม่ใช่เหตุการณ์ที่วิญญูชนโดยทั่วไปอาจล่วงรู้ได้

คำสำคัญ: การลักลอบขโมย หรือจารกรรมข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ การจารกรรมข้อมูลในโลกอินเทอร์เน็ต หรือการเจาะระบบข้อมูล ระดับความระมัดระวังตามสมควร การจารกรรมโดยวิธีไฮเทค

Abstract

The use of technology not only creates a number of advantages, but also entails risks and liabilities. Individuals who apply the technology must realize not only the advantages, but also their shortcomings. One of many possible causes of inefficiency in digital technology is the conduct of the signatories, relying parties, and certification authorities, as well as attacks by a third party. The acts of a third party, such as an impostor or a hacker, can be considered as offences in the use of digital signatures. The acts of stealing private key creation data may cause private key holders to sustain losses. Thefts can be instigated by means of copying private signing key creation data, stealing a smart card which contains a private key or hacking the signatory's computer hard-drive. Due to the highly technical nature of cyber stealing or hacking, the act of copying or hacking private keys stored in the signatory's hard drive may not be so obviously noticed or tracked as traditional theft or intrusion. The lay signatory may be unable to realize whether his private key has been copied or hacked. The standard of the reasonable man remains applicable in the use of digital signatures. A signatory is obliged to exercise due care as would be expected from a reasonable man who is in the same circumstances to avoid unauthorized use, access, theft or compromise of his private signature creation data. The signatory is also required to know apparent risks that a reasonable man would have known under a similar situation. High tech theft, however, is not an obviously apparent occurrence and a reasonable man would not know about it.

Keywords: Stealing Private Key Creation Data, Cyber Stealing, Hacking, Due Care, High Tech Theft

Introduction

The use of technology not only creates a number of advantages, but also entails risks and liabilities. No technology is ever absolutely perfect. Each technology has its unique benefits as well as its flaws. Individuals who apply the technology must realize not only the advantages, but also their shortcomings. The development of electronic commerce rests on trust in the identity of the transacting parties and the security of transmission and content of their communication (Barassi, 2002).

Parties to online transactions often consider security as an option, without realizing that it may sometimes be required by law.* The law does not require businesses to utilize specific security measures to transact with online users. Businesses implement transaction security measures in order to gain market share and to engender trust in online users.** Without proper security measures, businesses may be exposed to the risks of conducting transactions with impostors. Security policies are a crucial step in providing consumer protection from fraud. (Arnold et al., 2000). Thus, security will be the key to creating trust between parties conducting online business transactions (Smedinghoff, *supra* note 2, at 2.).

---

* Thomas J. Smedinghoff, *Securing Trust 1* (Feb. 1, 2002), at http://sprint.ziffdavis.com/ecommerce__1.html (last visited Nov. 1, 2002). For instance, the Federal Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d-2) requires healthcare providers to deploy security measures to ensure confidentiality and the integrity of healthcare information. Failure to comply with the regulation will result in penalties, including fines and possible imprisonment. In addition, under some laws in the United States, such as under the 1999 Illinois Electronic Commerce Security Act and the 1999 New York Electronic Signatures and Records Act and some laws of other countries such as the 1998 Singapore Electronic Transactions Act and the 2000 Hong Kong Electronic Transactions Ordinance, electronic signatures are enforceable in certain cases only if proper security measures are applied. For example, New York Electronic Signatures and Records Act § 540.4 (1999) provides that the signature that meets the criteria shall have the same validity and effect as the use of a signature affixed by hand. The signature has to be unique to the person using it, capable of verification, created using creation data under the sole control of the signatory, and associated with the electronic document in such a manner that authenticates the attachment of the signature to particular data and the integrity of the data transmitted. Thailand has adopted the Model Law on Electronic Signatures, approved by the United Nations in 2001. Under the Thai Electronic Transactions Act (2001), the enforceability of electronic signatures is based on their level of reliability.

** *See* LAW AND THE INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE 57(Lilian Edwards & Charlotte Waelde eds., 2000). A lack of consumer confidence is a major obstacle impeding the growth of e-commerce. The main risks which consumers encounter when they shop through the Internet are, for instance, that someone may use a consumer's credit card to make fraudulent purchases for which the consumer will be held accountable, and that the merchants will not perform their side of the contract or perform it defectively, and consumers fear being left without remedy or with a remedy that is difficult to enforce.

Signatories in Digitally Signed Transactions

A signatory or subscriber under the Model Law of Electronic Signatures is a person who holds signature creation data and acts either in his own capacity or on behalf of the person it represents. The Thai E-Transactions Act defines the signatory in a similar fashion to the Model Law. The E-Sign Act does not stipulate a definition for a signatory.*

A signatory under the E-Transactions Act means "a person that holds signature creation data and creates the electronic signature on his behalf or on behalf of the other person." A signatory of a digital signature is a person who possesses a digital signature creation data which he or she has exclusive control over the use of such signature creation data. The word signatory refers not only to natural persons, but also includes other entities, whether corporate or other legal persons,** which allow or assign a natural person to act on its behalf. For instance, a signatory can be an individual or a company acting through a natural person who applies the digital signature in the name of a company and binds the company as a principal under the law of agency.

Risks of Signatories in Digitally Signed Transactions

1. Risks of Relying on Unauthorized Digitally Signed Signatures

Guarding a private signing key is one of the most crucial issues in any Certification Authority-based system (Ellison, and Schneier, 2000). A private signing key may be used without authorization if a signatory does not

---

* *See* California Digital Signature Regulations (1998) § 22003 (a)(1)(K) provides that "subscriber" means a person who: is the subject listed in a certificate; accepts the certificate; and holds a private key which corresponds to a public key listed in that certificate. *See also* Utah Code Ann. § 46-3-103 (32)(1996) provides that "signer" means a person who creates a digital signature for a message. § 46-3-103 (33) (1996) stipulates that "subscriber" means a person who: (a) is the subject listed in a certificate; (b) accepts the certificate; and (c) holds a private key which corresponds to a public key listed in that certificate. *See also* Illinois Electronic Commerce Security Act § 1-105 (1998) provides that "subscriber" means a person who is the subject named or otherwise identified in a certificate, who controls a private key that corresponds to the public key listed in that certificate, and who is the person to whom digitally signed messages verified by reference to such certificate are to be attributed.

** UNCITRAL Working Group on Electronic Commerce, *Electronic Signatures: Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures,* 38th Sess., at 35.siv, U.N Doc.A/CN.9/WG.IV/WP.88 (2001).

maintain certain access control mechanisms for the protection of the private key.* For instance, if the signatory stores his or her private key on a conventional computer, the signatory must guard the private key with passwords or other authentication methods in order to verify the signatory's identity. Viruses and other malignant programs may also attack the private key creation data (Ellison & Schneier, *supra* note 10, at 2. *See also* FORD and Baum, 2000).

Even though a private key is protected by the use of passwords, the degree of security depends on how hard it is for a hacker to uncover such passwords. Such passwords should not be too easily guessed and the signatory should not use common words, as the potential of using a dictionary program to hack such passwords is enormous. If a private key is kept on a smart card where a microchip is used to store private key creation data, such smart card must possess attack-resistance attributes (Ellison & Schneier, *supra* note 10, at 2. *See also* FORD and Baum, 2000).

From a technical perspective, digital signatures are unbreakable, and it is impossible for a hacker to forge a signature.** In addition, digital signatures are not reproducible (Schneier, 2000). This makes it impossible for a forger to copy a digitally signed digital signature from one document and then paste onto another document. Repudiation of a digitally signed transaction is thereby rendered impossible. The weakest point of the digital signature lies in a compromise of the private key. Where this occurs there may be no discernable distinction between an authorized and unauthorized digitally signed transaction. The relying party cannot tell whether or not the signed message is genuine.

In order to maintain the trustworthiness of digital signatures, some states in the

---

* *See* I.C. PALMER & G.A. POTTER, COMPUTER SECURITY RISK MANAGEMENT 101(1999). The private key must always be protected by full password control. *See also* WARWICK FORD AND MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE OF DIGITAL SIGNATURE AND ENCRYPTION 129 (2000). To enhance the level of security, biometric technologies may be used to control access to the private signing key.

** *Id. See also* DANIEL MINOLI & EMMA MINOLI, WEB COMMERCE TECHNOLOGY HANDBOOK, SECURE ELECTRONIC TRANSACTION, INTERNET EDI, DIGITAL SIGNATURES 218(1997). A digital signature can only be created by someone who has knowledge of the private key. To verify the digital signature, it requires knowledge of the public key of the signatory. Other persons can only verify the digital signature, but cannot forge it.

United States, such as Utah* and Washington,** provide that the signatory is responsible for a digitally signed transaction whenever a certification authority certifies and approves the signatory's private key. This imposes a great burden on a signatory because the law does not care who uses such private key or what virus affects the signing (Ellison & Schneier, *supra* note 10, at 2.).***

In Thailand, the E-Transactions Act does not provide for either a presumption of validity of the digitally signed transaction or non-repudiation provisions. It leaves full discretion to courts to decide whether the digitally signed transaction was truly made by the signatory and whether the digital signature is reliable. The Act leaves leeway for a signatory to deny any unauthorized digitally signed transaction on the condition that the signatory maintained a reasonable standard of care in protecting his or her private key; otherwise, the signatory may be held responsible for such signing.

2. Possible Offences Concerning Digital Signatures

Most defects in the use of digital signature technology do not arise from the technology itself, but from the person who uses it. One of many possible causes of inefficiency in digital technology is the conduct of the signatories, relying parties, and certification authorities, as well as attacks by a third party.

A signatory usually prefers a simple and easy means of accessing his or her private key. For instance, the signatory may prefer a Single

---

* *See* Utah Code Ann. 46-3-406(3)(1996) stipulates "if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:
(a) that the digital signature is the digital signature of the subscriber listed in that certificate;
(b) that the digital signature was affixed by the signer with the intention of signing the message; and
(c) the recipient of that digital signature has no knowledge or notice that the signer:
(i) breached a duty as a subscriber; or
(ii) does not rightfully hold the private key used to affix the digital signature;..."

** *See* Washington Electronic Authentication Act § 19.34.350 (3)(1997) which provides that "if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:
(a) That digital signature is the digital signature of the subscriber listed in that certificate;
(b) That digital signature was affixed by that subscriber with the intention of signing the message;
(c) The message associated with the digital signature has not been altered since the signature was affixed; and
(d) The recipient of that digital signature has no knowledge or notice that the signer:
(i) Breached a duty as a subscriber; or
(ii) Does not rightfully hold the private key used to affix the digital signature."

*** *See also* Ford and Baum, 2000.

Sign-On in order to access private key creation data since he or she can access the signing key all day without the need to re-sign-on.* This makes access convenient, but it can make the digital signature technology unreliable. After the signatory has signed on, if he or she leaves the computer unattended for whatever reason, third parties are offered the opportunity to use the private key without the signatory's knowledge. Single Sign-On is not appropriate for digital signature technology because requiring a signatory to identify himself or herself each time before signing an electronic document ensures that each signing is authorized by the private key holder.**

A certification service provider that does not employ a high level of security technology in maintaining online certificates may give an opportunity to an impostor to access such certificate lists and add a phony certificate onto the list. This could make a relying party falsely believe that a person whose name appeared on the certificate list is really the person with whom he or she is contracting.

Before relying on digitally signed transactions, relying parties must inspect the Certificate Revocation Lists in order to make sure that a certificate issued by the certification authority has not been revoked. Failure to do so may be construed as negligence if in fact the certificate has become compromised or the certificate certifying the identity of a signatory is no longer valid, and may result in a substantial loss to the relying party.

The acts of a third party, such as an impostor or a hacker, can be considered as offences in the use of digital signatures. The acts of stealing private key creation data may cause private key holders to sustain losses. Thefts can be instigated by means of copying private signing key creation data, stealing a smart card which contains a private key or hacking the signatory's computer hard-drive. These are potential offences against which a signatory must take reasonable precautions.

A hacker may use a brute force attack to intrude or gain access to a private key as if he were an authorized private key holder. This act needs very advanced technology in order to break the cryptographic technology. It may also be possible in the near future for hackers to use highly advanced technologies to break codes or gain passwords in order to use private key creation data.

Other problems regarding the use of digital signatures are that the signatory may be forced into signing an electronic documents against his or her will, or the signatory may

---

* *See* note page 4.

** To eliminate repudiation issues, it is necessary that a signatory should verify himself or herself every time before affixing a digital signature to an electronic document.

be intellectually susceptible and manipulated into signing an electronic document against his or her interest (National Notary Association, A Position on Digital Signature Laws and Notarization, at 5, 2000).

Application of the Standard of Care in Case of High Tech Theft of Digital Signatures Creation Data

The use of digital signatures requires technical knowledge but it does not mean that the application of digital signatures requires professional skills. A layman who has received instructions on how to apply a digital signature would be able to use digital signatures properly. A signatory and relying party would need to learn how to apply and verify digital signatures. To ensure the highest degree of trust, it is necessary for the signatory, a key person in the use of digital signatures, to take proper precautions in safeguarding private creation data against unauthorized use, theft, loss or compromise. Digital signature technology is not an inherently dangerous technology; therefore, the person involved in the application of digital signatures is only required to possess due care.* Due care is ordinary care as would be expected from a reasonably prudent man under the same conditions and circumstances.

The test of ordinary care applicable to the signatory is an objective standard and the honest belief or best judgment of the signatory in keeping the private key secure is immaterial. The objective test is applied in order that

---

* *See* UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES art. 8(1)(a)(2001). "Where signature creation data can be used to create a signature that has legal effect, each signatory shall: exercise reasonable care to avoid unauthorized use of its signature creation data..." *See also* Utah Code Ann. § 46-3-305(1996) provides that (1) by accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate "assumes a duty to exercise reasonable care" to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature. *See also* California Government Code § 16.5. The signatory is required to retain control of the private key. The person who holds the key pair, or the subscriber identified in the certificate, "assumes a duty to exercise reasonable care" to retain control of the private key and prevent its disclosure to any person... *See also* Illinois Electronic Commerce Security Act § 10-125(1) and (2) (1998) which provides that "(1) the person generating or creating the signature device must do so in a trustworthy manner; (2) the signer and all other persons that rightfully have access to such signature device must exercise reasonable care to retain control and maintain the secrecy of the signature device, and to protect it from any unauthorized access, disclosure, or use, during the period when reliance on a signature created by such device is reasonable..." *See also* E-TRANSACTIONS ACT § 27(1) "In the case where signature creation data can be used to create a signature that has legal effect, each signatory shall: (1) exercise reasonable care to avoid unauthorized use of his signature creation data..."

relying parties and certification authorities can be adequately protected from the conduct of the signatory which is lower than the standard of the reasonable man in the same situation in safeguarding the private signing key against theft, loss or compromise. The imposition of protective measures on private creation data is indispensable. Leaving the private key unprotected or unattended may amount to negligence.

An example of an unreasonable conduct includes the act of writing a secret code on the reverse side of a smart card when the private signing key is stored in a smart card with pass phrase protection. In spite of the signatory's honest belief that sufficient care has been exercised in order to avoid other persons from gaining access to his private key, the act of writing the code on the back of the smart card or jotting down a password and leaving it in the vicinity of the smart card is unreasonable in the circumstances and may amount to negligence because a reasonable man, who is bound to keep a secret code, would not have written the code down.

Where the signatory is under a duty to report to persons who might rely on the digital signature that the private key has been lost, damaged, compromised or unduly disclosed, or that there is a substantial risk that the private key may have been lost, damaged, compromised, or unduly disclosed, he is obliged to report such circumstances as soon as he knows or should have known about the circumstances.* Otherwise, he will be held responsible to any relying party for damages. Whether he knows of the circumstances is the question of fact to be decided by a trier of fact or the jury. The court or the trier of fact needs to determine this question in the light of evidence.

The test of knowledge with respect to the reasonable man is based on an objective standard. The actor is required to know as a

---

* *See* Illinois Electronic Commerce Security Act § 20-110. "Except as otherwise provided by another applicable rule of law, if the private key corresponding to the public key listed in a valid certificate is lost, stolen, accessible to an unauthorized person, or otherwise compromised during the operational period of the certificate, a subscriber who has learned of the compromise must promptly request the issuing certification authority to revoke the certificate..." *See also* E-TRANSACTIONS ACT § 27(2) "Without delay, notify any person that may reasonably be expected to act on the basis of the electronic signature or to provide services in support of the electronic signature when: (a) the signatory knows or should have known that the signature creation data has been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with their purpose; (b) the signatory knows from the circumstances that there occurs a substantial risk that the signature creation data may have been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with their purpose..."

reasonable man would have known in the actor's place. Knowledge has been defined as a belief in the existence of a fact, which coincides with the truth (Prosser, 1971). Depending upon the circumstances, the actor must pay attention to his surroundings which a reasonable man would consider necessary and he must use such senses as he has to discover what is readily apparent (Prosser, 1971). The actor may be said to be negligent if he failed to look, or failed to observe what was visible when he looked* (Prosser, 1971). Any normal individual is assumed to know the traits of common animals, the normal habit and capacity of human beings, the danger involved in explosive materials, inflammable liquids, electricity, moving machinery, slippery surfaces, and firearms, including the fact that an automobile is hard to control in deep sand and that worn tires will blow out (Prosser, 1971). Since there is a minimum standard of knowledge that is based upon what is common to the community, the actor cannot be excused from liability when he denies knowledge of risk** (Prosser, 1971).

The objective standard applies to the concept of knowledge or what should be known in reporting the situation of substantial risk with respect to digital signatures. The court determines whether or not the signatory knows about the situation by comparing what a reasonable man would have known under similar circumstances. If the private signing creation data is stored in portable formats, such as a smart card, a reasonable man with ordinary prudence would have exercised proper care in inspecting his private key and would have known that the device which contains his private key creation data had been lost or stolen. If the smart card had been misplaced, lost or stolen, the signatory may be held negligent for not reporting the event if he failed to know or should have known the fact, as an ordinary person of reasonable prudence would. In other words, the signatory was not aware of things reasonably ascertainable upon inspection. Therefore, the conduct of a signatory who regularly uses his private key stored in the smart card but fails to inspect whether such key is still in his possession amounts to negligence.

Where the private signing creation data has been stored in a hard drive or smart card with additional password protection, such drive or card may have been copied or hacked. The use of additional protection measures to prevent anyone from unauthorized access is a reasonable conduct that might be expected

* The actor is required to see only where a reasonable man would do so.

** *See also* WILLIAM L. PROSSER ET AT., CASES AND MATERIALS ON TORTS 163(7th ed.1982). The reasonable person will not forget what he knows and the forgetfulness does not excuse negligence. However, lapse of time or other similar factors make it reasonable to forget and the actor may be excused from negligence.

from a reasonable man in protecting his private key data. There is still, however, a possibility of such protection being breached. The author is of the opinion that where the law requires the signatory to report situations where he knows or has reason to know or should have known about circumstances which might indicate high technological theft, an objective standard should be imposed on the signatory based on the knowledge of a reasonable person who is in the same situation.

The rationale in support of the external standard of knowledge in the notion of imposing a duty to report on the signatory is aimed at providing protection to third parties from relying on unauthorized digital signatures. The application of a subjective standard to the signatory's actual knowledge may create a substantial risk to the relying parties in the event where the signatory unreasonably failed to know of such circumstances. Although it places a great burden upon the signatory, the court will not hold the signatory liable if he has satisfied the standard of knowledge. From the author's perspective, the requirement of knowledge of high tech theft or compromise of the private key or a substantial risk involving the private key is based on an objective standard. The court has to take the conduct of the signatory and of a reasonable man under similar circumstances into consideration.* The signatory is bound to know certain facts as might be expected from a reasonable man who is in the signatory's position. If the signatory is a computer expert, he may know better than the person who is not. If a signatory is only a lay user, he may not know that his signature creation data has been copied or hacked since the hacker has used high technology in cracking the protection measures. In this case, the signatory may not be found negligent if the court is of the opinion that he has performed due care in acknowledging the occurrence of the unauthorized use, access, compromise of the private key as a reasonable lay user would have acknowledged, and the failure to be alerted of the circumstances is not so obvious that other reasonable signatories would have known in the circumstances (objectively).**

Due to the highly technical nature of cyber stealing or hacking, the act of copying or

---

* EDWARD J. KIONKA, TORTS IN A NUTSHELL: INJURIES TO PERSONS AND PROPERTY 131(1977). Epstein proposed the notion of double standard of conduct, namely, an external standard for a defendant's negligence, and a subjective standard for contributory negligence. However, his thesis is rejected; the result of the case is usually in favor of the plaintiffs because the application of the legal standard is left to the juries who tend to compensate the jury party.

** PROSSER, *supra* note 24, at 160. Meeting the minimum standard of knowledge, the individual will not be held to knowledge of risks which are not known or apparent to him.

hacking a private key stored in the signatory's hard drive may not be so obviously noticed or tracked as a traditional theft or intrusion. The lay signatory may be unable to realize whether his private key has been copied or hacked. Nevertheless, the computer expert or a person with computer skills would be able to investigate such a breach. A hypothetical person who is in the lay signatory's place would not have known about it. It can be concluded that the signatory who exercises due care to knowledge of hacking will not be held answerable for not knowing such risk which is not apparent to him.

There is no direct case regarding the duty to report the loss, compromise or theft of the private key, but such a proposition can be inferred from the following case. The court in Montgomery V. National Convoy & Trucking Co. (Montgomery V. National Convoy & Trucking Co., 1937) ruled that the defendant who failed to warn approaching vehicles of dangerous conditions was subject to liability. The court, in addition, noted that due to the ice on the highway, the defendant knew or should have known "the slippery conditions" and the defendant failed to provide a warning sign at the crest of the hill where it would be effective in warning approaching cars. Such failure not only amounted to negligence, but also to willfulness. The court applied the standard of a reasonable man to the defendant because the failure to provide a warning at a proper place would cause injuries to other users of the highway. The court stated that the defendant, as an ordinary person, knew or should have known where the sign should be posted in order to warn other approaching vehicles about conditions existing.

To draw an analogy between the duty to report key lost or compromise and the above case, the signatory is bound to notify other relying parties, just as the above defendant was obliged to warn the users of the highway. The court noted that providing a warning sign at the scene of an accident was inadequate in the circumstances because an ordinarily prudent person could not see the sign before reaching the crest of the hill. This was common knowledge which ordinary drivers knew or should have known.

The risk of high tech invasion or theft may be reasonably foreseeable for any computer users; however, the fact that the private signing creation data was copied or cracked by a high tech hacker may not be known to the signatory because high tech theft does not leave any track and the private signing creation data remains in the possession of the signatory even though the hacker has already acquired a copy of it. It is not common knowledge which ordinarily prudent users would have known. If the signatory's hard drive which stored the private key creation data has been infected or attacked by viruses or intruded by a hacker without the signatory's

actual knowledge, it is reasonable to assume that the signatory, as an ordinarily prudent user, would not have known about it. It is unfair to say that the signatory knows of something which he does not know. It is not similar to the case of "I didn't know the Edsel I sold you had no engine", since that is something that someone selling a car reasonably should know.*

It may be possible for the replying parties to argue that the signatory who kept the private key in the computer's hard drive should have installed an anti-virus program in order to detect any intruders. The failure to have such program would not be conclusive evidence for the court to hold the signatory negligent. The relying party, nonetheless, may adduce further evidence indicating the fact that the signatory subsequently detected that his hard drive has been infected by viruses or hacked by a hacker and failed to notify such events to the relying parties. Although he subjectively and reasonably believes that his private key is secure under the password protection, there are still reasonable grounds to believe that a breach of security measures may have occurred. The signatory is thus bound to notify such events despite his reasonable belief. If he fails to do so, he may be held responsible for his omission because, in the light of evidence, there is an obvious fact that the signatory should have known about the risks.**

Conclusion

In conclusion, the standard of a reasonable man remains applicable in the use of digital signatures. A signatory is obliged to exercise due care, as would be expected from a reasonable man who is in the same circumstances, to avoid unauthorized use, access, theft or compromise of his private signature creation data. The signatory is also required to know apparent risks that a reasonable man would have known under a similar situation. High tech theft, however, is not an obviously apparent occurrence and the reasonable man would not know about it. In the light of evidence, the signatory, nevertheless, may be held answerable for not notifying the relying parties of any substantial risk that the private signing creation data may have been copied or hacked, if in fact, it has been proven that the signatory had actually acquired such knowledge.

---

* *The Consumer Fraud Act, available at* http://public.findlaw.com/consumer/newcontent/consumerlaw/chp15__e.html (last visited July 10, 2003). The law will not allow parties who should have known something through the reasonable exercise of their senses and intelligence to fail to use them.

** *See Gobrecht v. Beckwith,* 82 N.H. 415, 420, 135 A. 20, 22 (1926). "Where a duty to use care is imposed and where knowledge is necessary to careful conduct, voluntary ignorance is equivalent to negligence."

References

Arnold, Tom, et al., eds. 2000. **Internet Identity Theft: a Tragedy for Victims.** Washington, DC: Software & Information Industry Association.

Barassi, Theodore Sedgwick. November 1, 2002. **The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions, American Bar Association** [Online]. Available : http://www.abanet.org/scitech/ec/cn/cybernote.html.

Edwards, Lilian, and Waelde, Charlotte, eds. 2000. **Law and the Internet : A Framework for Electronic Commerce.** Oxford : Hart Publishing.

Ellison, Carl, and Schneier, Bruce. 2000. **Ten Risks of PKI : What you are not Being Told About *Public Key Infrastructure,* 16 COMPUTER SECURITY J. 1, 1** [Online]. Available : http://www.counterpane.com/pki-risks.pdf.

Kionka, Edward J. 1977. **Torts in a Nutshell : Injuries to Persons and Property.** St. Paul, MN: West Publishing.

Montgomery, V. December 20, 2002. "National Convoy & Trucking Co., 186 S.C. 167, 195 S.E. 247 (1937)." **The Consumer Fraud Act** [Online]. Available : http://public.findlaw.com/consumer/newcontent/consumerlaw/chp15__e.html

National Notary Association. November 14, 2002. **A Position On Digital Signature Laws And Notarization, at 5** [Online]. Available : http://www.nationalnotary.org/Digitalsignature.pdf.

Schneier, Bruce. 2000. **Crypto-Gram** [Online]. Available : http://www.commons.somewhere.com/rre/2000/RRE.hacking.digital.sign.html

Smedinghoff, Thomas J. February 1, 2002, **Securing Trust 1** [Online]. Available : http://sprint.ziffdavis.com/ecommerce__1.html.

UncitraL Model Law on Electronic Signatures Art. 2(d) 2001. Vienna : Uncitral Secretariat.

Uncitral Working Group on Electronic Commerce. 2001. **Electronic Signatures: Draft Guide to Enactment of the Uncitral Model Law on Electronic Signatures, 38th Sess., at 35.siv, U.N Doc.A/CN.9/WG.IV/WP.88.** Vienna : Uncitral Secretariat.

Asst. Prof. Pongthon Somran received his Master of Law from Ramkhamhaeng University. He is currently Associate Dean for Academic Affairs of the School of Law, the University of the Thai Chamber of Commerce.