The Information Society Law : The Fusion of Law and Information Technology

Munenori Kitahara
Faculty of Economic Sciences, Hiroshima Shudo University
1-1Ozuka-Higashi 1-chome, Asaminami-ku, Hiroshima, JAPAN 731-3195

Abstract

In information society, legal norm communications have been never established in certain fields for a long time. That is, a few legal norms have never obeyed in the fields. Above all, legal norms which relate to data protection, information contents and information security, would often infringed. Most violation would be conducted by using information technologies. Information technologies would often be used in these infringing incidents. It can be said that these infringing incidents would have never been conducted without information technology. These infringing incidents include hacking actions, personal data abuse, personal information disclosure, unauthorized access, infringing copyrights, infringing privacy rights, and so on.

A way of preventing those infringements is to raise the level of punishment against the violators. But, it will prove to be disappointing. Furthermore, it would be an ex post facto measure to the last. It would be needed to invent an ex ante measure, if it is possible.

As the ex ante measure, the author proposes a fusion of law and information technology. An information technology will lead people to a lawful deed when they conduct actions in using computers and networks. They say that information technology cures information technology. After all, the collaboration will aim at realizing laws, and it will contribute to recover a social justice.

Key Words:

Fusion, Law, Information Technology, Information Ethics, IT Audit, Cloud Computing

1 Introduction

A few years ago, I tried to make up the system of information society law in Japan [1]. The legal system is composed of twelve legal groups (laws) and fifty two legal norms (acts). The information society law will form and run an advanced information and communications network society of the 21st century. The laws would regulate information (contents), information processing devices (computers), and information circulation routes (networks). In the society people live most of their information lives. Information life means a life where people use computers, the Internet, and information contents. They receive online administrative, financial, educational, commercial services on the Internet, or the Cloud.

In information society, the use of information technology has been recommended in order for individuals to exercise their legal rights. Both e-central government and e-local governments have promoted the use of information technology (PCs and the Internet) since the Law

Concerning the Use of Information and Telecommunications Technology on Administrative Procedures (Online Administrative Procedures Law) went into force in 2003[2].

On the other hand, they might meet across information accidents (computer crimes, cybercrimes). Information accidents mean informational incidents where internet users are infringed on their rights and profits. The accidents would include data protection right infringement, personal information abuse, privacy infringement, spoofing identity, tampering with data, repudiation, personal information disclosure, denial of service, elevation of privilege, copyright infringement, child pornography disclosure, and so on.

As described above, the information society has the legal system to prevent those unlawful incidents. Some legal norms, however, have never been complied with since the norms were established. In a part of the information society, legal norm communications would have not become established. It can be said that the legal norms as information have had no effectiveness.

Information accidents would mostly performed by using information technologies. They say that a computer virus is a kind of computer program. Computer misuse is the collective term for a number of criminal offences committed by means of a computer, often through access to the Internet [3]. The offences under a computer law are relevant to crimes involving the use of computers. Such offences can generally be distinguished into three categories. The first category is traditional type of criminal offence that may be committed using computers as the instrument of the crime. The second category concerns ‘content-related crimes’, where computers and networks are the instrument, but the content itself is illegal, such as infringing intellectual property and certain forms of pornography. The third category is offences that have been established to specifically address activities that attack the integrity, confidentiality, and availability of computer and communications systems, such as viruses and other malware [4].

Technologies would be neutral. This is as often the case with information technologies. A famous hacker was employed with his high information technology power by a big information provider. He had attacked the networks of the provider with information technology. The former hacker would try to protect the networks with the same information technologies as he had used to attack the networks. They say that like cures like. In other words, information technology cures information technology. The hacker's story could suggest that information technology could prevent unlawful actions with the same information technology.

Here, I can suggest some instances of a collaboration of law and information technology. The electronic signature act introduces a cryptographic technology to make it possible for anyone to make easy use of strict certification. The authenticity of any electromagnetic record can be legally verified by public key cryptosystem. The minor protection act shall oblige providers to apply a filtering and blocking technology to the child pornography information on the Internet. By implementing a data audit technology, a data controller can grasp a lifetime of personal data, which will contribute to the effectiveness of a data protection act. It might be possible to grasp personal data flow by attaching a logical IC tag to the personal data. The logical IC tag will play the same role as the header of an IP packet. ID of personal data will be presented on

the monitor of smart phones. Data subjects can know where and how their personal data are processed.

These examples mean a cooperative regulation of law and information technology. There can be found a collaboration of law and information technology in the cooperation. Information technology should be embedded into laws. But the laws should provide a security standard and structure standard of the information technology.

The fact, here, should be remarkable that those unlawful actions had been conducted with information technologies. Then, the information society law should introduce information technologies in order to recover the effectiveness of the law itself. This means that information technologies should regulate themselves in the law. This is a collaboration of law and information technology. The purpose of the collaboration is to realize the contents of laws by using information technologies.

Law enforcement agencies would use information technologies for policing, criminal justice. They have a combined research of criminal histories, available by entering a single request from a computer in a patrol vehicle, thus reducing radio traffic and a database can be required, resulting in more reliable crime analysis reporting or investigative searches. A system can link persons, addresses, property, and vehicles, thus reducing data entry and improving safety to the officer in the patrol vehicle[5].

As for the collaboration, there must exist some problems. The collaboration would compel people to use a specific information system. In addition, it must be misinterpreted that information technology would regulate information technology itself.

This paper has a few main goals. The first one is to show the examples of the collaboration of law and information technology in existing laws. The second one is to suggest the other possibility of the collaboration.

In this paper, I would like to propose a fusion of law and information technology. By introducing information technologies into laws, we can recover the legal effectiveness. That means realizing a social justice. A security and architecture standard of the information technologies which the laws provide. The structure and security standard of information technologies.

To reach the goals, I, first, will examine the uses of information technology in legal fields (2). Second, I will suggest that information technologies should include ethical elements (3). Third, I would like to show several examples of the fusion (4). Last, I will examine the security and architecture standard of information technology (5).

2 The Use of Information Technology in Law

2.1 Realizing Laws by Technology

Several years ago, miserable traffic accidents continuously occurred by large-sized trucks on the highway. The main reason was that the trucks ran at a tremendous speed and did not observe the legal speed. The road traffic act provides the maximum speed of trucks. In addition, the enforcement ordinance of the road transport vehicle act also provides the maximum speed

of 80 kilometers an hour. In these cases, both the act and the ordinance as information had no effect on the drivers.

Then the act required the large-sized trucks of installing the speed limiter. And the ordinance provided the security standard of the apparatus. The security standard provides that the speed limiter can adjust the supply of fuel for trucks not to exceed the speed of 90 kilometer per hour. The trucks must travel at the speed less than 90 kilometer an hour. All the trucks are also equipped with a tachometer which records speed.

This story suggests that the apparatus helped truck drivers to obey the legal speed on the highway. At the same time, it can be said that an act could recover the legal effect by technology. That is to say, this is realizing laws by technology.

2.2 Use of Information Technology in Law Enforcement

Increased computing power, advances in data transmission and attractive and user-friendly graphic interfaces present law enforcement agencies with unprecedented capacity to collect, store, analyze and share data with stakeholders inside and outside of government. Ultimately, information technology represents a tool to help local law enforcement achieve its broadened and increasingly complex mission [6]. Two areas in which information technology in policing has attracted a great deal of attention are crime mapping and information integration [7].

Today, law enforcement agencies have more technologies available to them than ever before. Information technology is a world of its own, and so is law enforcement. Marrying the two can result in a more efficient and, hopefully, safer working environment and community. Regardless of where technology is used, the activities in the agency's day-to-day business can be characterized as a business process. Applying information technology is not (and should not be) simply automating a process. It is using technology where it makes sense and brings about greater efficiencies [8].

2.3 Computer-Assisted Audit Information Technology

Information technology auditors gather evidence from an enterprise's books and records to support their conclusions. This audit evidence includes any actual paper-based documents, evidence that these documents or supporting transactions were properly recorded in a timely manner, and appropriate authorizing signature or notations. Today, most of those documents are IT based and paperless, and procedures to support their audit conclusions when older traditional paper-based documents have gone away.

IT auditors often need tools to better understand and evaluate the completeness accuracy of the data stored in the files and databases of IT applications. It is almost always more efficient to use information technologies to examine all recorded items on the supporting computer files [9].

An IT auditors must obtain evidence on the validity of accounting and operational data. IT audit approaches to testing, analyzing, and gathering detailed evidence from data contained on IT applications through the use of computer-assisted audit information technologies controlled by IT auditors. These technologies allow an IT auditor to review the contents of computerized applications data in files, ranging from accounting systems on large database repositories to

smaller systems residing on departmental desktop systems.

2.4 Information Technology Controlled with Information Technology

The infrastructures of information society are “information,” “information processing devices,” and “information circulation routes.” Software and contents technologies will relate to the information. Computer and machine technologies will relates to the devices. Networking and internet technologies will relate to the routes.

The information society law should introduce the information technologies in order to raise the effectiveness of the law itself. This introduction might be permitted only to the information society law. For example, electronic signatures acts introduce cryptographic techniques in order to make it possible for anyone to make easy use of strict certification functions using electronic certificates and to enable the safe supply and use of network services. An unauthorized computer access prevention act uses a firewall technology, which implements information security policies. And minor protection acts would oblige providers to apply a filtering or blocking technology to child pornography information on the Internet. This means that information technologies should control themselves in the law. It is really the fusion of technology and law.

3 IP Technology and Ethical Deed

3.1 Ethical Technology

The Internet is the only sphere that establishes ethics in itself by its own technology. A firewall router uses access control lists (ACL) and other methods to ensure the security of the private network. PAP (Password Authentication Protocol) that allows PPP peers to authenticate one another, does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PGP (Pretty Good Privacy) allows secure files and message exchanges. L. Lessig said that code is law [10]. I would say that code is ethics.

3.2 Ethical Deed and IP Technology

An end-user has nothing to do with the unlawful computer access and the computer virus. As the ethical deed, there is no way for the user other than constructing the firewall to the host computer or installing an anti-virus software. It is not possible to hope any more. If it is a timid user, it is already wax without becoming nature as for the Internet. However, the IP technology is offering a new technology. That is a quarantine network system. This system serves a severe authentication, and protects the user from the threat of unlawful computer access, virus and worms. People use the same password on different systems. People are going to rely less and less on passwords. So, a new password system is being developed.

Network administrators must be able to deny unwanted access to a network and allow authorized users to access necessary services. Security tools such as passwords, callback equipment, and physical security devices are helpful. However, they often lack the flexibility of basic traffic filters and the specific controls that most administrators prefer. For example, a network administrator may want to allow users access to the Internet, but not permit external

users Telnet access into the LAN.

Routers provide the capability to the filter traffic, such as blocking Internet traffic, with access control lists (ACLs). An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols. This module will introduce standard and extended ACLs as a way to control network traffic and explain how they are used as part of a security.

ACL technology can refuse the access from the networks and hosts which the sites think of undesirable. With the technology, the sites should limit the access right. Moreover, the sites could deny many processes (commands)—ping, telnet, http, ftp, and so on.

ACLs are also used in firewall routers. A firewall is an architectural structure that exists between the user and the outside world to protect the internal network from intruders. In most circumstances, intruders come from the global Internet and the thousands of remote networks that it interconnects. Typically, a network firewall consists of several different machines that work together to prevent unwanted and illegal access.

4 The Fusion of Law and Information Technology

4.1 Email Technology and Law

An email technology has been introduced into the Electronic Consumer Contracts Act. The article 2 (definitions) defines the electronic consumer contracts as follows:

"In this Act, an 'electronic consumer contract' means a contract that is made between a consumer and a business entity by electromagnetic method through a visual browser of a computer in cases where the consumer manifests his/her intention to make an offer or to accept the offer by transmitting his/her intention through his/her computer in accordance with the procedures prepared on this visual browser by the business entity or its designee."(1)

"In this Act, 'electromagnetic method' means a method using electronic information processing system or other types of information communication technology."(3)

"In this Act, 'electronic acceptance notice' means an acceptance notice to the offer of a contract which is, among electromagnetic methods, given by means of transmission through a telecommunication line connecting a computer, etc. (meaning a computer, a facsimile device, a telex or a telephone, the same shall apply hereinafter) used by the party dispatching the acceptance notice to the offer of the contract with a computer, etc. used by the offer or of the said contract."(4)

As described above, an electromagnetic method is using electronic information processing system or other types of information communications technology in this act. Transmitting offering and accepting electromagnetic records would use e-mail technologies.

The email technology uses SMTP (Simple Mail Transfer Protocol) and POP (Post Office Protocol) in TCP/IP.

A number of cryptosystems have been adapted to help secure e-mail, a notoriously insecure method of communication. Some of the more popular adaptations include Secure Multipurpose

Internet Mail Extensions (S/MIME), Pretty Enhanced Mail (PEM), and Pretty Good Privacy (PGP) [11].

S/MIME builds on the Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication via digital signatures based on public cryptosystems. PEM has been proposed by the IETF (Internet Engineering Task Force) as a standard that will function with public key cryptosystems [12].

4.2 Encryption Technology and Law

Encryption is one technique which can be used to achieve secrecy for the contents of a message, but there are other methods of hiding identities and information including steganography, remailers, account cloning and spoofing [13]. Encryption can provide confidentiality, integrity and authenticity of the information transferred countering the open nature of the electronic documents. Digital signatures can be created by the use of encryption, and these can authenticate the sender of the information.

The Electronic Signatures and Certification Business Act has introduced encryption technologies. The purpose of this Act is to provide the presumption of authentic establishment of electromagnetic records by electronic signatures. In the Act, any electromagnetic record that is made in order to express information shall be presumed to be established authentically if the electronic signature is performed by the principal with respect to information recorded in such electromagnetic record. The authenticity and electronic signature of the electromagnetic record can be verified by the public key cryptosystem.

Japanese electronic signatures act (Act on Electronic Signatures and Certification Business) has the following provisions:

Article 1(Purpose)

The purpose of this Act is to promote the distribution of information by electromagnetic forms and information processing through ensuring the smooth utilization of Electronic Signatures, and thereby to contribute to the improvement of the citizens' quality of life and the sound development of the national economy, by providing the presumption of authentic establishment of electromagnetic records, the accreditation system for designated certification businesses and other necessary matters, with respect to Electronic Signatures.

Article 2(Definitions)

(1) The term "Electronic Signature" as used in this Act means a measure taken with respect to information that can be recorded in an electromagnetic record (a record that is prepared by an electronic form, a magnetic form or any other form not perceivable by human senses and that is used for information processing by computers; hereinafter the same shall apply in this Act), and which falls under both of the following requirements:

(i) A measure to indicate that such information was created by the person who has taken such measure; and

(ii) A measure to confirm whether such information has been altered.

(2) The term "Certification Business" as used in this Act means a service that, in response to either the request of any person who uses the business (hereinafter referred to as the "User") with respect

to the Electronic Signature that he/she himself/herself performs or the request of another person, certifies that an item used to confirm that such User performed the Electronic Signature pertains to such User.

(3) The term "Specified Certification Business" as used in this Act means a Certification Business that, among Electronic Signatures, is performed with respect to an Electronic Signature that conforms to the criteria prescribed by ordinance of the competent minister as an Electronic Signature that can be performed by that person in response to the method thereof.

But, in these provisions, we can find no provisions to introduce an encryption technology into the act. The hint can be found in the ordinance for enforcement of the act (art. 2). That is, there is provided of the security of electronic signatures and the difficulty of electromagnetic records. In addition, the difficulty shall be depended upon the factorization in prime numbers of integer, and the calculation of discrete logarithm.

These hints suggest that we are forced to use an encryption technology in order to establish and send electromagnetic records.

The use of encryption seems to give rise to an element of suspicion - it is often assumed that the use of secret codes are associated with the world of spies and industrial espionage. Nevertheless, there are many legitimate purposes of secrecy in general and encryption in particular. Many are connected with business transactions and the desires to keep financial information away from the prying eyes of third parties and to authenticate and prevent repudiation of the communication as between the intended parties to the transaction. In this way, encryption technology is a fundamental element for the development of a global electronic commercial system [14].

4.3 Filtering Technology and Law

Packet filtering firewalls are simple networking devices that filter packets by examining every incoming and outgoing packet header. They can selectively filter packets based on values in the packet header, accepting or rejecting packets as needed. These devices can be configured to filter based on IP address, type of packet, port request, and/or other elements present in the packet [15].

In the Act Concerning Environment for Children to Safely Use the Internet, information providers shall be obliged to provide filtering technologies. This Act focuses on measures to protect minors from harmful information and explicitly provides for the direction of future efforts with respect to a vision of the environment for the Internet utilization.

4.4 Internet Technology and Law

The Internet is the only sphere that establishes a lawful action in itself by its own technology. A firewall router uses access control lists (ACLs) and other methods to ensure the security of the private network.

ACLs consist of the user access lists, matrices, and capability tables that govern the rights and privileges of users. ACLs can control access to file storage systems, software components, or network communication devices. In general ACLs can restrict access for a particular user, computer, time, duration--even a particular file. This specificity provides powerful control to the administrator [16].

Internet protocol security (IPSec) is an open source protocol that secures communications across IP-based networks such as LANs, WANs, and the Internet. The protocol is designed to protect data integrity, user confidentiality, and authenticity at the IP packet level. IPSec is the cryptographic authentication and encryption product of the IETF's IP Protocol Security Working Group [17].

PAP (Password Authentication Protocol) that allows PPP peers to authenticate one another, does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PGP (Pretty Good Privacy) allows secure files and message exchanges.

Pretty Good Privacy (PGP) is a hybrid cryptosystem originally designed in 1991. PGP combined some of the best available cryptographic algorithms to become the open source de facto standard for encryption and authentication of e-mail and file storage applications [18].

The Directive 95/46/EC requires that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

ICT offers solutions in the shape of privacy protection for users, consumers and citizens. The application of ICT to protect privacy has become widely known under the name Privacy-Enhancing Technologies (PETs). PETs have been defined as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data; all without losing the functionality of the data system. PETs are about technologies that enhance privacy and privacy protection is neither an equivalent of information security or confidentiality. PETs have to be used for implementing the legal specifications in the EU privacy directives, and can guarantee data protection without making excessive demands on the processing of the data. By applying PETs and streamlining personal data processing, the organizations can continue to meet the high public expectations with respect to services and dealing with personal data [19].

4.5 Data Audit Technology and Law

By implementing a data audit technology, a data controller can grasp a lifetime of personal data, which will contribute to the effectiveness of a data protection act. It might be possible to grasp a personal data flow by attaching a logical IC tag to the personal data. The logical IC tag will play the same role as the header of an IP packet.

Packet filtering firewalls examine every incoming packet header and can selectively filter packets based on header information such as destination address, packet type, and other key information. The firewalls scan network data packets looking for compliance with or violation of the rules of the firewall’s database [20].

4.6 Email Filtering Technology and Law

SaaS for email primarily involves cleaning spam, phishing emails, and malware included in email from an organization’s incoming email stream, and then delivering that clean email security to the organization so that it is effectively not repolluted [21].

This is accomplished by using either Secure Socket Layer (SSL) or Transport Layer Security (TLS) on network communications at the transport layer [22].

4.7 Web Content Filtering Technology and Law

In the Cloud, a SaaS provider scans for malware threats and ensures that only clean traffic is delivered to end users. SaaS providers supplement that URL filtering with the examination of HTTP header information, page content, and embedded links to better understand site content. SaaS for web content also involves scanning outbound web traffic for sensitive information (e.g., ID numbers, credit card information, intellectual property) that users could send externally without appropriate authorization (data leakage protection). Web traffic is also scanned for content analysis, file type, and pattern matching to prevent data exfiltration [23].

Content filter effectively protects the organization's systems from misuse and unintentional denial-of-service conditions. A content filter is a software program or a hardware/software appliance that allows administrators to restrict content that comes into a network. The most common application of a content filter is the restriction of access to Web sites with nonbusiness-related material, such as pornography or entertainment. Another application is the restriction of spam e-mail from outside sources. Content filters can consist of small add-on software for the home or office, or major corporate applications [24].

Content filters ensure that employees are not using network resources inappropriately. Unfortunately, these systems require extensive configuration and constant updating of the list of unacceptable destinations or incoming restricted e-mail source addresses. Some newer content filtering applications update the restricted databases automatically, in the same way that some antivirus programs do. These applications match either a list of disapproved or approved Web sites, for example, or key content words, such as *nude* and *sex*. Content creators, of course, work to bypass such restrictions by suppressing these trip words, creating additional problems for networking and security professionals [25].

4.8 Cloud Computing Technology and Law

Information processing systems which include personal information should be required of a privacy design in the architecture. Cloud technologies provide the privacy design. It should be included in the checklists of privacy impact assessment.

It is important to consider how users approach an application architecture for systems that have a special segment of private data, notably e-commerce systems store credit cards and health care systems with health data. The key to privacy in the cloud -- or any other environment -- is the strict separation of sensitive data from nonsensitive data followed by encryption of sensitive elements [26].

4.9 Authorizing Technology and Law

In 1999 the Unauthorized Computer Access Prohibition Act was established in Japan. The Act provides the punishment of unauthorized computer access and the security measures of access controllers. An unauthorized computer access means an act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via a telecommunication line, any information or command that can

evade the restrictions placed by that access control function on that specific use (art.3(2)), and an act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication line, any information or command that can evade the restrictions connected (art.3(3)).

The access controller who has added an access control function to a specific computer shall endeavor to properly manage identification codes relating to that access control function and codes used to confirm such identification codes through that access control function, and shall always verify the effectiveness of that access control function, and, when he deems it necessary, shall endeavor to promptly take necessary measures to protect that specific computer from acts of unauthorized computer access, including the upgrading of the access control function concerned (art.5).

Then the access controllers will be required of necessary measures to protect the specific computer systems.

4.10 Architecture Technology and Law

The security controllers must start security measures from the outside (perimeter) of an operating system and work toward the center not to leave servers and hosts unprotected. With an initial perimeter layer implemented, the controllers at least have one umbrella layer of security in place, which is much better than having nothing at all [27].

This layered approach is to develop a layered security posture, or defense-in-depth. Layers are important because they add levels of protection. If one layer is breached, the controllers have multiple layers beneath it to continue protecting their valuable assets. For example, if an attacker manages to compromise the firewall, they still have IDS (Intrusion Detection System) and host security to protect them from a full network compromise. This gives them the opportunity to focus their efforts on the firewall issue instead of worrying about what other systems have been compromised [28].

5 The Security and Architecture Standard of Information Technology

5.1 The Security Standard of ICTs

Biometric systems are increasingly being considered as better fool-proof methods of ensuring security in several areas ranging from national security to credit card processing, as opposed to traditional methods such as alphanumeric passwords and personal identification numbers [29].

The Biometric Consortium is to develop widely acceptable standards for the application level and device level interfaces that are independent of the operating systems and vendors, and to be able to support a variety of biometric applications. Due to the sensitivity of information contained in biometric systems, it is expected that such systems will be attacked by intruders both from within and outside the country [30].

5.2 The Architecture Standard of ICTs

Assurance and security mechanisms need to be provided for the information stored in the

biometric systems both in stored and transit modes. It is important to understand the design principle underlying the architecture and management of biometric systems so that appropriate mechanisms can be used to secure such systems.

In order to maximize the level of security provided buy biometric systems, multimodal systems are being considered as better alternatives to relying on a single biometric for identification and verification purposes. Multimodal biometric systems utilize multiple signatures of the same individuals obtained from different sensors. Information (signatures) obtained from multiple sensors can be fused together to improve the performance of identification and verification systems and compensate for lack of sufficient features from the signature obtained from a single sensor. Information fusion can take place while extracting features, while matching the scores obtained from different modalities, or while making decisions. Results obtained from information fusion suggest that the reliability of biometric systems can be significantly improved by combining two or more biometric signatures [31].

5.3 The Necessity of the Standards

The users of these information technologies which are installed in laws are the addressees of each law. The addressees have duty to comply with laws. They would use these information technologies when they conclude contracts and conduct administrative processes. Most of the addressees normally have little knowledge of the technologies. This, first of all, must be taken into consideration in introducing the collaboration of law and information technologies.

Therefore, those ICTs would be required the security and the architecture standards. A security level of technologies must be assured, and the architecture level must be based on the security level. The success of the collaboration needs an ICTs impact assessment in order to look for the standards. At least a privacy impact assessment will have to be conducted [32].

Information technologies are also being used for law enforcement, that is, for policing. The using purpose might be completely different from that of the collaboration. But, the authority recognizes that information systems are indispensable tools for effective, expedient, and well-informed policing [33].

In addition, it also recognizes that technology also poses an enormous security risk. Law enforcement agencies that operate mission-critical information technology systems without adequate security controls in place put the public, themselves, and the government at extreme risk. Data contained within these systems are extraordinarily sensitive and mission-critical. Sensitive case reports, confidential investigative data, agency intelligence, suspect and personal data, and personnel information are just a few examples of data that may be subject to compromise via a malicious hack, an untrustworthy insider, an accidental misuse of the system, and /or a natural disaster [34].

Creating security policies and instituting a security process has traditionally been an afterthought in many IT implementations. Too often, only marginal consideration is given to the security of a system when it is being developed or implemented. What is missing is the adoption of an IT security policy development process, a conscious decision by senior management to establish a formal procedure to investigate and analyze the very real security

risks to the agency's IT systems, and to develop mechanisms and policies designed to mitigate those risks. Securing an information system is much more involved than merely requiring a password, applying a digital signature, or using encryption. It is organizational strategy that must be driven by the highest levels of the organization [35].

6 Conclusion

This paper would mainly aim at collaborating law and information technology. That is to say, laws might use information technology for a legal system to become effective. I would like to borrow the functions of information technologies. Or, if I say marrying law and information technology, is it an overstatement?

The important features of computer systems are adopted in many social systems in the information society. Because the computer systems are by nature political and social.

Information security technology includes authentication technology, data protection technology and information filtering technology. These technologies would require the users of an ethical consideration. These technologies might lead the users to an ethical deed. Therefore, I would define that these information technologies are ethical technologies.

It will be permitted that these technologies are used to realize the contents of laws in place of the laws, because the technologies are political, social and ethical. That is, this is the collaboration of law and information technology. The collaboration will aim at realizing social justice.

There might be certainly various problems about the collaboration. First, technologies will regulate technologies. Second, the collaboration will force the users to use specific computer systems with the information technologies implemented. Third, the collaboration will have to cope with the evolution of technologies. Last, there will be left the problem of standardizing the technologies.

Information society, increasingly, depends on computer systems to behave acceptably in applications with extremely critical requirements, by which she means that the failure of systems to meet their requirements may result in serious consequences.

There is good news and there is bad news. The good news is that computer system technology is advancing. Given well-defined and reasonably modest requirements, talented and diligent people, enlightened and altruistic management, adequate financial and physical resources can be built that are likely to satisfy certain stringent requirements most of the time. The bad news is that guaranteed system behavior is impossible to achieve. There can always be circumstances beyond anyone's control. Besides, people are fallible. Thus, there are always inherent risks in relying on computer systems operating under critical requirements [36].

The law must evolve to reflect how both society and technology evolve, for the truth is that neither the tech-deterministic school nor the socially-mediated school is completely correct. The information society is rooted in connections between people enabled by, and mediated by, digital technology [37].

References

[1] See, M. Kitahara, Information Society Law in Japan, *US-CHINA LAW REVIEW* Vol.8, No.1, 2011, pp,21-40.

[2]The MPMHT, 2003 White Paper, p.62.

[3] Andrew Murray, *Information Technology Law: The Law and Society*, Oxford Univ. Press 2010, p.327.

[4]See, C.Reed/J.Angel(eds.), Computer Law, 6th ed., Oxford 2007, pp.553-554.

[5]See, National Law Enforcement and Corrections Technology Center, *A Guide for Applying Information Technology in Law Enforcement*, U.S. Department of Justice 2001, p.1.

[6] Kent Reichert, Use of Information Technology by Law Enforcement, Dec. 2001, pp.1-4. (http://www.sas.upenn.edu/jerrylee/programs/fjc/paper_dec01.pdf)

[7] Ibid.

[8] National Law Enforcement and Corrections Technology Center, ibd., pp.1-2.

[9] R.R.Moeller, *IT Audit, Control, and Security*, WILEY 2010, p.304.

[10] Lawrence Lessig, *Code (Version2.0)*, Basic Books 2006, p.5.

[11] M.E.Whitman/H.J.Mattord, *Management of Information Security*, 2nd ed., THOMSON 2008, p.384.

[12] Ibid.

[13] Y. Akdeniz/C. Walker/D.Wall(eds.), *The Internet, Law and Society*, Longman 2000, p.320.

[14] Ibid., p.321.

[15] M.E.Whitman/H.J.Mattord, *Management of Information Security*, 2nd ed., THOMSON 2008, p.353.

[16] M.E.Whitman/H.J.Mattord, *Principles of Information Security*, 3rd ed., Course Technology 2009, pp.181- 183.

[17] Ibid., p.388.

[18] Ibid., p.390.

[19] S.Gutwirth/Y.Poullet/P.D. Hert/R.Leenes (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Springer 2011, pp.309ff.

[20] M.E.Whitman/H.J.Mattord, *Principles of Information Security*, 3rd ed., Course Technology 2009, pp. 245- 246.

[21] Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'REILLY 2009, p.220.

[22] Ibid.

[23] M.E.Whitman/H.J.Mattord, *Reading and Cases in the Management of Information Security*, Course Technology 2006, p.63.

[24] M.E.Whitman/H.J.Mattord, *Management of Information Security*, 2nd ed., THOMSON 2008, p.373.

[25] Ibid.

[26] G. Reese, *Cloud Application Architectures*, O'Reilly 2009, pp. 80ff.

[27] M. Andress, *Surviving Security: How to Integrate People, Process, and Technology,*

SAMS 2002, pp.26-27.
[28] M. Andress, ibid., p.25.
[29] M.E.Whitman/H.J.Mattord, *Management of Information Security*, 2nd ed., THOMSON 2008, p.64.
[30] Ibid.
[31] M.E.Whitman/H.J.Mattord, *Principles of Information Security*, 3rd ed., Course Technology 209, pp. 340ff.
[32] See, Office of the Privacy Commissioner (Australian government), *Privacy Impact Assessment Guide*, 2006.
[33] COPS (U.S. Department of Justice), *Law Enforcement Tech Guide for Information Technology Security : How to Assess Risk and Establish Effective Policies*, 2006, p.3.
[34] Ibid.
[35] Ibid.
[36] P.G.Neumann, *Computer Related Risks*, Acm Press 1995, p.4.
[37] Andrew Murray, ibid., p.574.