# INFORMATION SECURITY IN THE NETWORK AGE*

*Kazuko Otani***

## LIGHT AND SHADOW OF THE NETWORK AGE

There is a famous comic character named *Doraemon* for children in Japan. Doraemon is a visitor from the future, a robot shaped like a cat living in a child's closet. Doraemon makes fun of people living in current society by some devices brought with him from the future. A miracle door named *Dokodemo Door* is one of such devices that may be set anywhere and can bring people anywhere they wish to go only by opening the door. The Dokodemo Door reminds us of the vision designed by the information superhighway.

Vice President Al Gore proposed the information superhighway in the *National Information Infrastructure (NII) Agenda for Action* presented on 15 September 1993, aiming to revitalize the United States of America's national industry, create new employment, strengthen the competitive power and for other purposes. The plan showed a vision of the near future in which all information concerning education, medical affairs, entertainment and administrative services will be available to anybody without being affected by birthplace, sex, religion, geographical distance and other handicaps.[1]

---

*Paper presented as part of the proceedings of THE 1995 ANNUAL MEETING OF THE RESEARCH COMMITTEE ON SOCIOLOGY OF LAW, International Sociological Association, 1-4 August 1995, The University of Tokyo, Tokyo, Japan.

**Assistant Manager, Legal Affairs Department, The Japan Research Institute, Limited.

[1]U.S. NII TASK FORCE, THE NII AGENDA FOR ACTION (1993).

The *Internet*,[2] spreading all over the world, makes the dream of the Dokodemo Door even closer and advances the concept presented by the NII and the Global Information Infrastructure (GII). Simply by connecting to the Net and opening the window of your home computer, you may send information to the world and communicate with people living on the other side of the Earth. The Internet is different from the telephone network, which is now the sole widespread telecommunication network, in conquering the gap of not only distance but also time. It is similar to the telephone on the point that any information will immediately arrive at the address. It is likewise similar to mail on the point that the addressees do not have to wait at home to receive the arrival of the information. Additionally, like broadcast, you can send any information to the public and search any information from all libraries connected to the Net without being required to do anything other than operate a personal computer. Some excellent freeware, such as MOSAIC[3] is available for computer and telecommunication non-professionals to access the World Wide Web (WWW)[4]. If you open the home page[5] of the White House, for instance, you will find a portrait of the Presidential family and hear the mewing of Socks, the family pet.

Undoubtedly, the era of networking has come, when we depend on plural information systems connected to each other. But amidst the bright side of the era of networking, we also find

---

[2]The *Internet* is a decentralized network interconnected by the TCP/IP protocol. The Net was started as a military network *ARPANET* in 1969 by the US Department of Defense for the purpose of networking main frame computers to prepare against missile weapons. It opened to public research organizations and universities in 1983 and has been interconnected with commercial networks since 1990.

[3]*MOSAIC* is a computer program developed by Illinois University, providing human interface to browse through the WWW free of charge.

[4]*WW: World Wide Web*, the information searching system developed in Europe, allows access to data bases via Internet all over the world. MOSAIC has a role of guidance for WWW.

[5]The *home page* is an electronic entrance for visitors to an organization connected to Internet, providing publicity and guidance to help them access any information which they want to get.

shadows in the form of pornography and information infringing other people's reputation or privacy distributed on the Internet. Surely and steadily, the Internet is becoming a risky space; many passwords to access important systems, credit card numbers and trade secrets have been stolen and sold in underground markets.[6] As Mr. E. Cohen, a famous security expert put it, "tapping the Internet is easier than tapping a telephone."[7]

Thus, we pay the compensation of risk for the concept of Dokodemo Door.

*Technological Innovation and Limit of Law*

Apart from the US Government, which first promoted the GII, other countries have also began working on articulating the position for preparation of a high level information infrastructure concerning institutional, legal and technical issues.[8]

The current boom related to multi-media is undividedly connected to this information highway concept. The NII is led by *AT&T, BT, NTT* and other common carriers of telecommunications infrastructure; however, the multimedia boom is promoted by companies manufacturing computers, operating systems, software, processor chips and audio-visual games. If you compare the information highway to the traditional highway, the former is the owner of the road and the latter will be the manufacturers of automobiles. Recent marked innovation in the field of computers and communication technology[9] has made multi-media possible,

---

[6]In the underground market, there are crimes such as money laundering and other illegal transactions. See *The Hot News concerning Computer Crime in the US, the Paradise of the Hacker--Internet is Popularized*, Nikkei-sangyo-shimbun, 18 April 1995.

[7]See Nikkei Computer, 11 July 1994.

[8]Nikkei-shimbun, 27 February 1995.

[9]*MPEG* (Moving Picture Experts Group), the international technical standard of ISO and IEC regarding compressing and expanding of moving pictures, has made moving pictures recorded in CD-ROM playback. *ATM* (Asynchronous Transfer Mode) is the remarkable telecommunication method to unify various sizes of information into homogenous cells to be sent rapidly.

because multi-media requires enough capacity to treat numerous data efficiently.

However, we are faced with further problems in operating reliable networks which may provide high level applications in both aspects of quality and quantity. These problems are as follows:

> (1) preparation of a seamless telecommunication network infrastructure that can answer many kinds of needs;
>
> (2) preparation of conditions for creating and distributing contents of high quality;
>
> (3) promotion of creators who can use computers;
>
> (4) preparation of rules that are well-balanced between protecting intellectual property, including copyrights, and encouraging use of property; security against the risk of masquerade or tampering and improper or unauthorized access to information; and standardization for sharing technical results; and

(5) preparation of the organizational issues for shifting to paperless accounting documents and applying that to administrative services, such as patent applications, customs formalities, electronic records of patients, and remote consultation on medical affairs.

Some of the aforementioned problems will be resolved by technical innovation or wise industrial policy, but some problems require legal consideration. This report intends to show the latter issues. The law is always trying to catch up with things. Recent technical innovation has shaken the traditional legal system to its foundation. One anachronism of the legal system is remarkably found in copyright protection, because the Copyright Act was enacted when traditional works were created and used based on an analog technique. Recent digital works require the revision of the concept of "copy" in the existing copyright system.[10]

---

[10]*A Preliminary Draft of the Report of the Working Group on Intellectual Property* is the US Green Paper drafted by IP/WG represented by Bruce A.

*Information Security*

Before analyzing risks concerning information security and network reliability, we must look for the causes and the places affected by such causes. The causes are generally called *threats* in some information security criteria. And in places affected by these causes, we have to find the *vulnerability* of information systems. Deborah Russel and G.T. Gangemi suggested in their books that when the vulnerability of the information system encounters a threat, it needs the countermeasure of security.[11]

*Threats against Information System and Networking*

A. Natural Disaster

The big earthquake which struck Kobe City and the Hanshin-Awaji region on 17 January 1995 has shown the weakness of the information network as well as its importance. The circuit voice telecommunications has a capacity for double congestion, but then, the congestion was fifty times normal. The serious breakdown of the information network, including the wireless system made it impossible for organizations such as fire departments and police to grasp what happened in the stricken region and caused a fatal delay in rescue. But other than earthquakes, floods, lightning damage, rat infestion, snow damages and the combinations thereof are also experienced.

---

Lehman (Assistant Secretary of Commerce and Commissioner of Patents and Trademarks) and NII Task Force Chairman Ronald H. Brown (Secretary of Commerce) in July, 1994. In Europe, the members of the High-Level Group on the Information Society, headed by Michael Bangemann, drafted the *Recommendations to the European Council* (also known as the "Bangemann Report") on Europe and the Global Information Society.

[11]Computer Society Basics (1991).

B. Man-made Accidents

These include war, terrorism,[12] fire, data congestion, emanation smog, failure of electrical power,[13] hardware breakdown and software bugs, breakdowns of telecommunication circuits, failure of maintenance or operation.[14]

C. Criminal Action

Some examples are physical destruction, unauthorized altering and tampering, improper data input, computer viruses,[15] use of networks by unauthorized users such as *crackers*,[16] masquerade, eavesdropping, tapping, and blocking or denying services.

Vulnerability of the Network

We must understand not only the threats to the network but also its own vulnerability. A software named *SATAN: Security Analysis Tool for Auditing Networks* has been distributed in the Internet and has a function to find any weak points or flaws of a

---

[12]The World Trade Center (WTC) Bomb Terror in February 1993 killed and injured over 1,000 people, and companies doing business in the WTC took all of two months to recover totally. Before recovery, they did business with back-up computer centers, but many companies were worried over ensuring back-up space.

[13]The fire occurred at the New York Transformer Substation in August 1990 and stopped power in the region of South Manhattan. Most financial institutions extended their closing time and could accomplish processing on the same day, although any company using the PBX (Private Branch Exchange) could not make any calls.

[14]The Setagaya Cable Fire occurred in November 1984 owing to an error during maintenance operations.

[15]*Computer Virus*, a kind of computer program showing symptoms of infection which appear after being hidden in other programs, may destroy data, application programs or operating systems, or stop processing in the infected computer. Various types of viruses are known and vaccine programs to find virus programs and delete them have been developed. The estimated damage of the Internet Worm Case in November 1988 amounted to US$97 million.

[16]In this report, a *cracker* means a computer fanatic who enjoys accessing and invading computer systems by all means.

specific network. The vulnerabilities of networks, other than those attributable to users, may be traced to (a) public switched network and other communications circuit equipment, (b) computer hardware, (c) software, (d) media, and (e) failure of electric power.

Analysis of Damage or Loss

The following types of loss will occur when threat and vulnerability are encountered:

*(1) Direct damage against the systems*

The remedy for damage against systems should be one of the critical issues when the equipment or facilities might be destroyed physically and stop working, such as the cost for installing cable, repairing the broken facilities, buying new equipment, re-inputting data, developing software, and so on.

*(2) Denial of services*

The question of who shall bear the cost and expense for alternative measures during the suspension of service, damages owing to denial of service and so on is important.

In the famous *Internet Worm Case* on 2 November 1988, which is known as the first case in which a criminal has been prosecuted and convicted by applying the Computer Fraud and Abuse Act[17] one worm program self-reproduced and increased from one computer system to others until it occupied the memory of over 1,000 computers infected by the worm. No one could work their computer systems until they recovered the systems after many hours and much labor. The estimated damage was between US$10-100 million for labor costs to restore the system, though no system was destroyed or broken.

[17] Revised 18 U.S.C., Sec. 1030 (1986).

*(3) Lost profit*

Owing to a cable fire in Setagayu-ku, Tokyo in 1984, owners of food shops who were providers of delivery service on call have claimed from the telecommunications carrier their lost profits during the stoppage of their business due to denial of service. As a result of the action, it was determined that they should not be indemnified and NTT (the telephone company) was not liable for the accident. The value of the case, nevertheless, lay on its showing the dependence of present men's daily lives on the information network.

*(4) Lost data*

It is difficult to estimate and verify the value of lost data. Some computer virus can attack anytime and delete all the stored data, including the operating system and other programs, after displaying a Christmas message or playing some music like Yankee Doodle.

*(5) Invasion of privacy*

Some *crackers* enjoy trespassing and browsing through a computer system without stealing or detroying the target system, though they leave most owners of invaded systems in the same unpleasant state as when their houses were invaded. Some authorized users of subscription bulletin board systems (BBS) may disclose private information about other users without the latter's approval. Attention should be given to two pending cases[18] tackling the question of whether or not any BBS operator should be liable for misuse by its users.

*(6) Trade secrets and Intellectual Property*

As the KGB spy case shows, trade secrets, highly-classified national secrets and intellectual property on networks may be

[18]See Mainichi-shimbun, 22 April and 18 May 1994.

aimed at. It is a fact that widespread Internet has brought computer crime close to us. A stolen quotation price by a competitor has caused a contractor to fail in competitive bidding. In the underground market, stolen trade secrets and credit card numbers are traded as commodities. An angry hacker has withdrawn from an account opened by a consultant who published the existence of such underground markets. But reported cases are only the tip of the iceberg of total accidents because such weaknesses are always kept concealed.

*(7) Unfair profit by fraud or abuse of system*

*(8) Expanded damage (network risk)*

We must prepare for an expansion of damage caused by accidents occurring on other interconnected networks. The BCCI case, showing the effects of time differences, teaches us of the threats of network risk. An emergency or contingency plan will be effective, but it is necessary for operators of interconnected systems to share information and to cooperate in preparing emergency plans against the common risk.

***The Definition of Security***

Subject to the idea suggested in the Security Guidelines for information systems adopted by the Organization for Economic Cooperation and Development (OECD), *security* means the countermeasures to protect the interest of people who rely on information systems from the risk caused by the lack of availability, integrity and confidentiality. Before opened networks, symbolized by the Internet spread, most concerns were paid to the stable operation of the system, keeping information in confidence and protecting facilities from physical destruction. It is essential for a closed and centralized system to control access to facilities and network. That is still important but is no longer enough in the Network Age. Today's networks--each of which developed in accordance with its own purpose--are reciprocally interconnected, and users who access the network also have specific purposes.

This, therefore, all the more highlights the importance of security against threats to the integrity of the information system. In this regard, the NII Security Issues Forum of the US provide as follows:

*integrity* -- assuring that information will not be accidentally or maliciously altered or destroyed;

*reliability* -- assuring that systems will perform consistently and at an acceptable level of quality;

*availability* -- assuring that information and communication services will be ready for use when expected;

*confidentiality* -- assuring that information will be kept secret, with access limited to appropriate persons.

***Criteria or Principles for Security***

The criteria or principles vary according to the nature of systems and needs of their users. Most of such criteria are stated by a defensive approach. The purpose of criteria is generally to prevent the actualization of potential risk and to minimize the loss and damage arising out of the risk. The important criteria are as follows:

**International Criteria or Standards**

* Security Guideline of Information Systems adopted by OECD (1992)

* ITU-TS (CCITT: *Comite Consultatif Internationale Telegraphique et Telephonique*, until 1993) and ISO (International Standards Organization) are working on the problem of security

* ITSEC (Information Technology Security Evaluation Criteria) by the German Information Security Agency (GISA), 1992, known as the "White Book" in Europe

**U.S. Criteria or Principles**

* Five Tenets for Security by NII Security Issues Forum (1995)

* TCSEC (Trusted Computer System Evaluation Criteria) by the National Computer Security Center (NCSC), 1987, known as the "Orange Book"

**Japanese Criteria**

* National Computer Policy (NCP), 1972

* Criteria for Computer System Security by the Ministry of International Trade and Industry (MITI) of Japan, 1977

* Regulation of Authorized Data Processing Center Performing Security by MITI, 1981

* Security Reliability Criteria of Information and Telecommunications Networks by the Ministry of Posts and Telecommunications, 1987

*Technology for Security*

The Trusted Network Interpretation of the Trusted Computer Systems Evaluation Criteria, or the so-called "Red Book", categorizes many security services into classes of integrity of telecommunication data, denial of service and prevention of divulgence, and states a brief evaluation of them.

It is difficult to talk about integrity of telecommunications data without mentioning the innovation of cryptography techniques. Cryptography has made it possible to shift from a defensive to an offensive approach. Applications of cryptography are not only limited to keeping the contents in confidence even if an omission or divulgence has occurred. Use of cryptography also prevents masquerade, fraud and tampering and it provides a good tool for authentication, such as digital signature, applying the public key encryption technique developed in 1976.

***Legal Considerations***

As we have examined the analysis and procedure for security with two approaches--public criteria and technology--the next issue relates to the legal responsibility for loss or damage arising out of actualization of risk from the lack of security.

Some rules related to transactional security

Some organizations and governments have tried to discuss the rules for transactional security, including risk of loss, such as security procedures provided in the US Uniform Code of Commerce[19] and the Draft Model Statutory Provisions on the Legal Aspects of the EDI in UNCITRAL.[20] Both rules involve the idea of suggesting the legal effect of an agreement between the parties to a transaction, which is on condition that if one party implements an agreed security procedure, such party shall be indemnified from all

---

[19]U.C.C.4A, Section 201, defines *Security Procedure* as a procedure established by agreement of a customer and a receiving bank for the purpose of:

(i) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or

(ii) detecting error in the transmission or the content of the payment order or communication.

[20]*Draft Model Statutory Provisions on the Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Data Communication*, UNCITRAL (United Nations Commission on International Trade Law) A/CN.9/WG.IV/WP/62:

*Article 7*, [Functional equivalent][Requirement] of "signature":(1) Whereas a rule of law requires information to be signed or provides for certain consequences if it is not, that requirement shall be satisfied in relation to a data [record] containing the requisite information if:

[(a) a method [of authentication] identifying the originator of the data [record] and indicating the originator's approval of the information contained therein has been agreed between the originator and the addressee of the data [record] and that method has been used; or]

(b) a method [of authentication] is used to identify the originator of the data [record] and to indicate the originator's approval of the information contained therein; and

(c) the method was as reliable as was appropriate for the purpose for which the data [record] was [generated or communicated] [made], in the light of all circumstances [including any agreement between the originator and the addressee of the data [record]].

loss or damage arising out of the transaction. It is one of resolution by a civil law approach to risk of loss.

However, there is some apprehension with the application of this rule between unequal parties, as between a bank and its depositor, for instance. The depositor might have a one-sided disadvantage in relation to the bank, which operates a black box system safe from the scrutiny of the depositor and other customers. In such cases, the following four conditions may be necessary to ensure that transactional security takes advantage over individual loss:

> (1) Both parties should agree by free will and without compulsion.
>
> (2) Both parties should share or have access to equal information necessary to enter into an agreement.
>
> (3) Both parties should know and acknowledge the contents of the security procedure and each party's role in implementing such procedure upon agreement.
>
> (4) The procedure agreed upon must meet international standards for security procedures as to identification, message authentication, availability, accuracy, the non-repudiation rule, integrity, and others.

The security procedure must be reasonable in consideration of the technological level and cost requirements. However, the cost consideration should not be so emphasized in cases involving the users' lives, bodies and property, such as in medical systems. The security of transaction policy should be accompanied by a consumer protection policy.[21]

---

[21]The Electronic Fund Transfer (EFT) Act of 1978 covers a wide variety of EFTs, including consumer transactions. U.C.C.4A, Section 108, provides for the exclusion of consumer transactions governed by Federal Law. The EFT Act shall be applied to retail transactions, while the Uniform Commercial Code--Funds Transfer shall be applied to wholesale wire transfers.

Criminal law

Many countries have enacted or revised their criminal law systems, incorporating thereto penal laws to address computer crimes. In Japan, the Criminal Code was revised in 1986 to protect the reliability of electromagnetic records to the same degree as paper documents.[22] But at that time, provisions regarding new types of crime, such as unauthorized access or use of computer systems, theft of computer time and production of computer viruses, were put off. After the revision, an organization that deals with information security (JIPDEC) discussed the schema of punishment for such crimes as unauthorized access.[23] Under such circumstances, what should be protected as a legal interest is a critical issue. The reliability or the integrity of data processing supported by computer systems should be protected. Subject to the Multidisciplinary Principle[24] of the Nine Principles of the OECD, it cannot absolutely be said that all acts producing risk against integrity should be made criminal offenses. Other methods or procedures, such as education or a technical approach, should still be effective.

Certainly, the U.K. Computer Misuse Act enacted in 1990 has defined unauthorized access to computer materials as criminal in that jurisdiction. However, there is yet to be a consensus on this conclusion. Under the US Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030(a)(5)) in 1986, the mere use of computer hours is not illegal.[25] Unauthorized access to the Federal interest computer system and obtaining anything of value is illegal. The NII Security Issues Forum has proposed in the latest report, *NII Security: The Federal Role*, that the aforementioned Act should be extended to

---

[22]Some of these provisions of the Criminal Code are: Articles 2(5), 7-2, 157.1, 158.1, 161-2, 234-2, 258 and 259.

[23]See *Criminal Law Measures regarding Illegal Acts against Information System*, Japan Information Processing Development Center (1990).

[24]Multidisciplinary Principles recommend us to consider related aspects, including technology, administration, organization, procedure, commerce, education, law and other disciplines for security of information systems.

[25]18 U.S.C. Sec. 1030.

protect all United States Government and financial institution computers and be applied to computers used in foreign communications, not just interstate communications. The report said the "these and other changes must be made to ensure that law keeps pace with new technology." In this light, resolution of the problems by criminal law should be limited to concrete and explicit threats against availability, confidentiality and integrity. Criminal conduct should not be extended to acts of abstract and obscure risk.[26]

*Extent of tort liability*

It is a critical issue if system operators should be liable for tort in the network operated by them In the case of *Playboy Enterprises, Inc. v. George Frena, Techs Warehouse BBS Systems and Consulting, and Mark Dyess,*[27] the court found that "Defendant Frena's unauthorized display and distribution of PEI's copyrighted material is copyright infringement under 17 U.S.C. Sec. 501." In Japan, there are two actions[28] regarding injury reputation and disclosing private matters in dispute related to the accountability of a BBS operator. Both operating companies are arguing against the plaintiff on the ground of secrecy of communication. These issues are complicated because of the conflict between two legal interests: secrecy of communication and individual rights, such as privacy. At this point, it is necessary to monitor and control misuse of BBS from the view of public interest on condition that there is express agreement between users and operators to do so. But such operator's role of control and monitoring the network should not be extended to non-public communications such as person-to-person communication. Secrecy of communication and freedom of speech and expression take precedence over other interests.

---

[26]Craig Niedorf was prosecuted for disclosing the structure of E911 system on his BBS. However, the system has been opened to the public. *See* D.E. Dening, *United States vs. Craig Niedorf--A debate on Electronic Publishing, Constitutional Rights and Hacking,* in 34 CACM 22-32 (March 1991).

[27]89 F. Supp. 1552 (M.D.Fla. 1993).

[28]*See* note 18, *infra.*

*Merger of communication and broadcast*

Thus far, new services have been provided by operators using network resources. Some communication services like BBS are merging with broadcast media. It is also a critical issue to place these new services located on the borderline between network communications and broadcasting to their respective places within the legal system, considering the difference between the traditional character of broadcasting and telecommunications and the tendency of merging media services.[29]

## CONCLUSION

In the conclusion of this report, because of the technological innovation in the field of computers and communications, the necessity of dealing with legal considerations is readily seen. However, the author proposes that no legal scheme should injure the good character of the Network Age, as symbolized by the Dokodemo Door, by intending to keep pace with technological innovation. We must endeavor to find a consensus in the society of the Network Age before we revise the civil, criminal and business law aspects of our legal systems.

---

[29]The tendency of new merging services involves the following:

(1) Digitalization and band broadening which have caused broadcasting and telecommunications to share circuits such as CATV, FM wave, communications satellites and other networks; and

(2) New services such as BBS and special broadcast channels being located at the midpoint of communications and broadcasting--the former as communication opened to the public and the latter as broadcasting provided to limited receivers.