Procedural Justice

Changes in Social Structures in an Information Society
and the Maintenance of Justice

Takato Natsui

Attorney and Professor, Meiji University Faculty of Law

Both before the Internet era and today, there has been a key concept in the preserving and maintenance of justice. It is control against the "compulsory collection of information."

The most typical example of this would be the preservation of due process of law in criminal proceedings through the prohibition of forced self incrimination, the exclusion of hearsay evidence, and procedures concerning searches and seizures by warrant as provided for in both the Constitution and the Criminal Procedure Law. These provide for certain procedures when the state acting as a criminal investigator can forcibly collect information from individuals based on its authority. These procedures are relatively complex and burdensome. The formulation of these procedures, however, is intended to maintain a reasonable balance between the justice of performing criminal investigations and the justice of maintaining the privacy of the individual. Additionally, by making the investigation procedures themselves objective and reasonable, they are intended to exclude evidence that does not reflect reality and prevent conduct by investigating authorities that violates human rights.

There is a reason why due process is given a prominent place in the Constitution. This is because in the era before the Internet, the only body that could in effectively exercise compulsory authority was the state. In such a time, it was sufficient to devise legal innovations to restrain the exercise of compulsory power within a reasonable scope. This is the historical and social dynamic that exists behind the guarantee of due process.

In the information society that has developed since the advent of the Internet, however, a significant change is taking place in the reciprocal relationship of this social dynamic.

It has become commonplace, for example, for Internet service providers (ISPs) and other companies to use monitoring software, video monitors, and other means to monitor the content of user communications and for ordinary companies to monitor constantly the conduct of employees and customers. In addition, many companies collect and store personal information concerning their customers in databases. Also, the music and film industries use Digital Right Management (DRM) system[1] to trace and monitor the conduct of customers who purchase their products. All of these actions are taken by private companies, not the state. In addition, we can discover many spy software (spyware) in our computer systems. Such software can retrieve, obtain, collect our important data or information and send it to someone stealthily, as well as trace, observe our behavior on the Web and send results of such tracing and observation to someone in secret.

[1] High Level Group on Digital Rights Management, Final Report
http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/index_en.htm

Many of these types of actions correspond to retaliation (as a kind of illegal self-defense that is prohibited by law). For example, the introduction of large volumes of dummy data into a P2P network to prevent the proper operation of the P2P software is conduct that interferes with business and exceeds the scope of permissible self-defense.

Using electronic technologies to access the computers of each individual without consent in order to ensure the security of information and protect copyrighted works is no more than unjust conduct. Even if such conduct were taken as a form of lawful self-defense or out of necessity, when the grounds for self-defense or necessity do not exist, or they no longer exist, information should be provided to the individual whose computer was accessed, but there is no such theory or practice in existence today. Consequently, this type of conduct should be deemed simply unauthorized access and unlawful conduct.

Even if monitoring on networks by private corporations is performed automatically by technological means, it is in effect the compulsory or forcible collection of personal information from individuals. Looking at it objectively, this conduct bears no relationship to the forcible investigatory activities undertaken by police and other government agencies. Since the “effective forcible monitoring” and the “effective forcible information gathering” conduct of private companies is not forcible action taken by the state, the due process guarantees provided by the Constitution and the Criminal Procedure Law do not directly apply to such conducts in the private sector.

That is to say, ordinary citizens have the opportunity to enjoy the controls on the forcible information collecting activities of the state as provided by the Constitution and the Criminal Procedure Law. In contrast, in the overwhelming majority of instances, the individual has no opportunity to exercise any appropriate controls on the forcible information gathering activities that are handled by private companies.

Of course, there are countries where the prior consent of the individual is required by law to collect personal information especially in democratic countries. In such countries, the individual has opportunities to control the forcible collection of personal information without consent by private corporations (e.g. EU personal data protection directive and some related legislation in European countries[2]). Such examples, however, are relatively rare. The number of persons who are aware of these issues concerning the forcible collection of personal information by private companies is small among legal scholars, let alone corporate managers and information security law specialists.

This is an extremely unfortunate situation. There have been several significant developments concerning this issue; however that provides hints about how it can be approached. For example, the Guidelines for the Security[3] adopted by the OECD in 2002 provide the following as one fundamental principle of information security.

---

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
http://europa.eu.int/comm/internal_market/privacy/law_en.htm

[3] the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
http://www.oecd.org/dataoecd/16/22/15582260.pdf

5) Democracy
The security of information systems and networks should be compatible with essential values of a democratic society.
Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

This provision does not make any specific and explicit reference to due process of law. It does provide, however, that security should be implemented in a manner consistent with the values recognised by democratic societies. It is clear that the guarantee of due process is considered one of the most important values of a democratic society. Consequently, security structures must be created and employed in a way that they are compatible with due process.

These guidelines concern security. And these guidelines may indeed have little to do with other matters. Nonetheless, the recommended fundamental principles established by the guidelines should be applied to all types of transactions that take place on the Internet including those that involve matters other than security. This is true, for example, with regard to the inclusion and application of DRM technology for the protection of copyrighted musical works. The obligation for music users to be monitored by music companies, unilaterally and without their knowledge, is contrary to justice in all respects. In this area too, procedural due process must be carried out.

As mentioned earlier, the concept of due process guarantees in the private sector is one that has not been considered at any length in the past. In the post-Internet information society, however, not only the state, but private corporations as well can effectively engage in the forcible collection of personal information. As a result, we must search for and consider means that will allow individual to exercise controls on the collection of information and will make it possible to enjoy procedural justice in the private sector too.