The growing market value of personal data and the difficulty of maintaining information privacy in cyberspace have prompted the legal experts to devise an alternative legal framework for effective data protection. This paper discusses some such alternatives available in the literature under intellectual property rights regime. Tensions between data protection and intellectual property rights enforcement are also mentioned briefly.

**Keywords:** Personal data, data privacy, information privacy, data protection, intellectual property, moral rights, trade secrecy.

Definitions of privacy vary widely according to context and environment. In many countries, privacy is interpreted in terms of management of personal information or ‘data protection’. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person’s affairs. The recognition of privacy is deeply rooted in history. Various countries developed specific protections for privacy in the centuries that followed.

Privacy can be divided into the following separate, but related, concepts:

(i) Information privacy, which involves the establishment of rules governing the collection and handling of personal data. It is also known as data protection;

(ii) Bodily privacy, which concerns the protection of people’s physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;

(iii) Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and

(iv) Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space and includes searches, video surveillance and ID checks.

Personal data are any information that directly or indirectly allows the identification of individuals it refers to and may include contact data such as name, mailing and e-mail addresses, telephone number, etc.; credit information; medical records covering medical and genetic information of the patients; government or public records containing tax identification number or an individual’s social security number. The automobile registration database is also a good source of personal data, so are the insurance policy records and bank records. The WHOIS database of the Internet Corporation for Assigned Names and Numbers (ICANN) contains identification information of domain name registrants. Some service providers may even use logos, images, and other media assets or create templates and computer programming pertaining to their clients. There could be umpteen number of sources of personal data.

Personal data have become an economic resource that many businesses need and use for the supply of their products and services. In the light of these developments a number of solutions are advanced in the literature for providing greater protection to personal data in cyberspace and elsewhere. Discussions at various fora have been taking place to consider whether the law should play a greater role in promoting greater information privacy in general and in cyberspace in particular. Both economic and non-economic considerations, which favour greater protection for personal data, have been put forward. Only property rights-related proposals are discussed in this paper.

**Privacy and Intellectual Property Issues**

Data management and safekeeping of the customer and employee information are fundamental to the well-being of corporations today, especially since customer information is one of the most valuable
assets of most companies. However, policies for data protection may also have the unintended consequence of hampering efforts to enforce intellectual property rights. Tensions between data protection and intellectual property rights enforcement have surfaced in debates and litigation over how much access should be allowed to ICANN’s WHOIS database. In many countries, rules on the protection of privacy permeate many aspects of business activity, including the protection and licensing of intellectual property rights. Personal data may be easily collected using new technologies without the person being aware and thereafter sold, licensed or used to create new intellectual property-protected products. Such data are incorporated in databases and, thereafter, licensed as part of a broader intellectual property package. Personal data may be needed for research/study programmes, for instance, in the medical field, where the results are expected to be protected by intellectual property rights (patent or copyright mainly). Personal data are indispensable information for Internet-based services as well.

Legal Protection of Personal Data

In many countries around the world, there is a general law that governs the collection, use and dissemination of personal information by both, the public and private sectors. An oversight body then ensures compliance. This is the preferred model for most countries adopting data protection laws. The genesis of modern legislation in this area, i.e., specific rules governing the collection and handling of personal information, can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978). In fact, Europe is on the cutting edge of regulation--especially when it comes to data privacy.

Two crucial international instruments evolved from these laws: The Council of Europe’s (CoE) 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, and the Organization for Economic Cooperation and Development’s (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, set out specific rules covering the handling of electronic data. These rules describe personal information as data that are given protection at every step from collection to storage and dissemination. The expression of data protection in various declarations and laws varies. However, all require that personal information must be:

(i) obtained fairly and lawfully;
(ii) used only for the original specified purpose;
(iii) adequate, relevant and not excessive to purpose;
(iv) accurate and up to date;
(v) accessible to the subject;
(vi) kept secure; and
(vii) destroyed after its purpose is completed. These two agreements have had a profound effect on the enactment of laws around the world. Nearly thirty countries have signed the CoE Convention and several others are planning to do so shortly. The OECD guidelines have also been widely used in national legislation, even outside the OECD member countries. The International Chamber of Commerce’s (ICC) Commission on E-Business, Information Technology and Telecoms has produced the ICC Privacy Toolkit.

The privacy laws and data protection laws in the United States and around the world pose numerous and difficult challenges to businesses. The applicable laws and regulations are complex and new ones are enacted frequently. Consumer focus and media scrutiny of privacy issues make this a very visible and high risk area for most businesses. Specially, information privacy is a scarce commodity in cyberspace. The technical infrastructure of cyberspace makes it remarkably easy and cheap to collect substantial amounts of information identifiable to particular individuals. Once these data have been collected, information technologies make it very easy and cheap to process the data in any number of ways. The market incentives for firms to collect and process personal data are very high. Data about users is not only useful in assessing how a firm might improve its service for its customers, but it also has become a key commercial asset which firms use both for internal marketing purposes and for licensing to third parties. The company gains the full benefit of using the information in its own marketing efforts or in the fee it receives when it sells the information to third parties.

New Property Rights Approach of Protection

While the companies are reaping full benefit of using customers’ personal information in its own
marketing efforts or in the fee it receives when it sells the information, customers often do not learn of the over disclosure of their personal data. They may not be able to discipline such companies effectively. Moreover, it can be daunting for an individual consumer to bargain with such companies. To overcome this market failure, in recent years, a number of economists and legal commentators have proposed that the law should grant individuals a property right in their personal data which would enable individuals to bargain over their personal data. Others have recommended a contractual approach to protecting personal data. Some suggest that the law should try to facilitate the privacy agreement the two sides would reach if they were both well informed and it was not expensive to reach an agreement. Arguments in favour of granting individuals property-related rights in their personal data available in the literature can be divided into three models: (i) intellectual property rights, (ii) moral rights, and (iii) trade secrecy.

**Intellectual Property Rights Model**

It may seem natural for individuals to assume that they do or should own data about themselves. It is surely true that the law will enforce the expectations of individuals that certain private information should remain secret. As Individuals generally have a legal right to exclude other people from access to their private data, they may have a sense that they have a property right in the data as well as a legal right to restrict access to it. Even when data about individuals are in the hands of others, individuals may perceive themselves to have a protectable interest in records of their financial transactions or medical histories. The law sometimes protects these and other types of data from unauthorized uses and disclosures which may also reinforce the sense of ownership in personal data. However, the rationale for these legal protections has not been grounded on a perception that people have property rights in personal data as such.

Experts have proposed that the law should grant individuals a property right in their personal data which would enable them to bargain over which personal data to reveal to which firms and for what purposes. They favour propertizing personal data as a way to allow individuals to make appropriate deals for selling their personal data and to receive compensation for use of their personal data so that markets in personal information will work more fairly. A property rights model offers two principal benefits: First, it would establish a right in individuals to sell their personal data and thereby capture some of the value their data have in the marketplace. Second, a property rights model would force companies to internalize certain social costs now borne by others from the widespread collection and use of personal data. Perhaps firms would collect or process less personal data than they currently do if they have to pay individuals for rights to do so. If so, this would simultaneously achieve information privacy goals and allow individuals who wish to sell their data to receive some benefits from this market.

This approach to personal data protection would, in essence, establish a new form of intellectual property right in information. It would be an intellectual property right of a very different sort than the one provided by the existing regimes. Intellectual property law grants exclusive rights in information-based creations in order to promote development of a thriving marketplace for them. A number of legal experts have observed that in an information economy, it seems almost inevitable that information will increasingly be commodified and new property rights will be created. Granting individuals property rights in their data would seem to be consistent with this general trend and the emergence of an ‘attention economy’ (the economy of cyberspace). A property-rights approach to solving the information privacy problem presumes that people by and large will be willing to disclose their personal data to businesses and allow them to use these data as long as the individuals obtain a discernible benefit from this disclosure and use. This approach may be especially useful to accommodate the varying preferences of individuals about private sector uses of personal data. A property-rights approach offers a further potential advantage over other legal approaches to protecting privacy in that it could protect personal data without requiring the establishment of a substantial government bureaucracy, as some nations have done to oversee regulation of personal data protection.

Despite these appealing features, a serious mismatch is reported between the traditional rationale for granting property protection to an information resource and the rationale for granting individual property rights in personal data. Also mismatched are traditional policies of property law favouring free alienability and information privacy policy preferences for restrictions on alienation. That is, collectors of data may prefer a default rule allowing
them to freely transfer personal data to whomever they wish on whatever terms they can negotiate with their future buyers. However, individuals concerned with information privacy will generally want a default rule prohibiting retransfer of the data unless separate permission is negotiated. If the goals and mechanisms of property law are misaligned with information privacy policy objectives, protecting privacy as intellectual property simply may not work. A few examples of such mismatch are: (i) The most common justification for granting property rights—to enable market allocations of scarce resources—does not seem to apply to personal data. What is scarce is information privacy, not personal data. If anything, personal data are being too plentifully distributed in the marketplace right now. Indeed, a reason many people argue in favour of granting individuals property rights in these data is, in essence, to make their distribution scarcer, (ii) The personal data most likely to become the subject matter of such a property right, for the most part, already exist. Property rights are not needed to bring them into being, nor to achieve their widespread distribution, (iii) The creation and dissemination of personal data do not generally promote ‘science’, i.e., knowledge, nor do they promote technological innovation. Thus, the purpose of the proposed new personal data property right seems almost the inverse of traditional intellectual property law, for it would grant a property right in order to restrict the flow of personal data to achieve privacy goals.

Creating a property right in personal data may, moreover, be objectionable to those who consider information privacy to be a fundamental civil right. The civil right conception of personal data protection is predominant in Europe. From a civil liberties perspective, propertizing personal information as a way of achieving information privacy goals may be viewed as an unnecessary and possibly dangerous way to achieve information privacy goals.

Moral Rights Model

A few experts are of the opinion that, as a model for a non-traditional property rights, ‘moral rights’ of authors might be adaptable to protecting personal data. In Europe and many other nations, authors have ‘moral rights’ in the works they have created. These rights are distinct from the purely economic rights that European law grants to authors. The moral rights regime derives from a conception of artistic and literary creations as emanations of the author’s personality in which he can and should retain an interest even after copies of the work have entered the stream of commerce. Among the commonly recognized moral rights are the rights of attribution, i.e., the right to be identified as the author of the work, and the rights of integrity, i.e., the right to protect the work from alterations that would be harmful to the authors’ reputation. In some jurisdictions, authors also have moral rights of ‘divulgation’, i.e., the right to decide when and under what circumstances to divulge the work, and sometimes even of withdrawal, i.e., the right to withdraw all published copies of the work if the work no longer represents the author’s views or otherwise would be detrimental to the author’s reputation. Moral rights are generally waivable by contract. An advantage of moral rights is that these rights can be exercised long after the author has sold copies of the work to the public and can be exercised against remote purchasers. While moral rights generally focus on the personal, reputational interests of authors, an economic consideration may partly underlie moral rights.

Moral rights-like approach might be worth considering for personal data. As with the moral rights of authors, the granting of moral rights to individuals in their personal data might protect personality-based interests that individuals have in their own data.

The admixture of personal and economic interests could be reflected in the right. The integrity and divulgation interests may be the closest analogous moral rights that might be adaptable to protect personal data. An individual has an integrity interest in the accuracy and other qualitative aspects of personal data, even when the data are in the hands of third parties. An individual also has an interest in deciding what information to divulge, to whom and under what circumstances. However, the idea of creating moral rights-like interest in personal data may have its own difficulties.

Trade Secrecy Model

Modified trade secrecy default rules for promoting information privacy is yet another proposal in respect of personal data protection. Trade secrets encompass various types of business information, whether technical, commercial, financial, which is not known or readily ascertainable by the relevant public and which gives a business a competitive edge (for
instance, manufacturing processes, techniques and know-how, customers’ lists and profiles, distribution methods, financial information, ingredients, etc). In general, information is eligible for trade secret protection if it is identified, substantial and secret, as reflected in Article 39 of TRIPS Agreement. A trade secret can be used as a competitive advantage for an unlimited duration as long as it remains secret. Unlike patents, trademarks and copyrights, which are regulated by federal law, trade secrets are regulated by state laws. Each individual state has its own unique trade secret law. The United States is one of the very few countries where civil protection against trade secret misappropriation is provided expressly by the Uniform Trade Secrets Act (UTSA), enacted by 43 states. The law can grant individuals a protectable interest in their personal data by setting a default rule forbidding certain activities with respect to these data, such as unauthorized collection or uses of them unless the individual has agreed to these activities.

The general rule of trade secrecy licensing law is that if the licensor has provided data to another for a particular purpose, the data cannot be used for other purposes without obtaining permission for the new uses. Although trade secrecy and information privacy laws obviously differ in many significant respects, these laws, nonetheless, have at least three important interests in common:

(i) protecting the interest of the claimant to restrict access to and unauthorized uses of secret/private information;
(ii) giving firms/individuals control over commercial exploitations of secret/private information, and
(iii) setting and enforcing minimum standards of commercial morality. To achieve policy goals embodied in these interests, trade secrecy law has evolved a set of default licensing rules. Some of these default rules may be adaptable to the licensing of personal information and information privacy protection.

Conclusion

At the moment, there is a vibrant market in personal data, a strange market in which owners of such data play a very small role. Many firms collect and process personal data because these are valuable. Besides, information technology makes it easy and cheap to gather and use them. In a number of instances, the law does not generally recognize the legal right of an individual to control uses or disclosures of personal data. Perhaps, at present, personal data owners have no legal right to stop firms from marketing their personal data to other firms. Nor can they stop governments from selling data available in the public records about themselves. Although the law often protects the interests of individuals against wrongful uses or disclosures of personal data, the rationale for these legal protections has not been grounded on a perception that people have property rights in their personal data as such. Privacy is a social goal; which may be achieved through social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data.

However, little thought has been given so far about how to move from where we are today to a thriving market in personal data under a property rights regime in which individuals would have a right to control market transactions in data about themselves. It is indeed difficult to design a legal regime which protects interests of all stakeholders appropriately. The task of devising a workable legal framework for regulating private sector uses of personal data is obviously very difficult if one takes a multi-dimensional perspective on the nature of a person’s interest in personal data. Even, at present, it is difficult for the average person to judge the risks of selling his/her property rights in personal data. Government should adopt a flexible and responsive approach to the protection of personal data, including the acceptance of property rights-related solutions. Work must continue on evolving norms about appropriate and inappropriate uses of personal data. Perhaps a nontraditional (sui generis) form of intellectual property rights deserves a consideration.

References

3 Samuelson Pamela, Privacy as intellectual property? www.sims.berkeley.edu/~pam/papers/privasip_draft.pdf