

CHAPTER 2

DATA PROTECTION AND TRANSBORDER DATA FLOWS: BALANCING PROPRIETARY AND PRIVACY RIGHTS

David C. Gryce and Roxanne A. Esch
Arent Fox, PLLC
Washington, D.C., United States

2.01 Introduction

(a) In General

The tremendous increase in transborder data flows and the existence of international data banks which are used in everything from the processing of the most mundane daily tasks to the creation of the most advanced information products reflects the increasing dependence on digital information resources. They also highlight the need for harmonization of national policies seeking to encourage the unencumbered flow of information and the need to balanced proprietary rights in the data against the right to restrict the collection, processing, and dissemination of data that is of a personal nature.¹

The free flow of information is important because it diffuses, throughout the world, innovative ideas and technology — two critical ingredients of economic growth.² Through human endeavor, these two ingredients are

1 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 430.

2 “The New Economy: Beyond Hype — The OECD Growth Project”, 2001 *Gen. Econ. & Future Stud.* 9, at p. 41 (July 2001).

transformed into new innovations and technological developments, forming the primary fuel for future development.³

National policies must encourage and support the development and diffusion of new innovations throughout the world economy, and one of the primary ways policy makers can ensure the generation and gain of new knowledge is by establishing proper incentives for innovation, such as those created through intellectual property rights regimes.⁴

While the Organization for Economic Cooperation and Development (OECD) recognized early on that national policies should establish standards along with incentives for innovation, it also recognized the value of and began establishing guidelines for the protection of privacy in the context of transborder flows of personal data. The OECD is made up of:

30 member countries [who share] a commitment to democratic government and the market economy With active relationships with some 70 other countries, NGOs, and civil society, it has a global reach The OECD produces internationally agreed instruments, decisions and recommendations to promote rules of the game in areas where multilateral agreement is necessary for individual countries to make progress in a globalize economy For more than 40 years, the OECD has been one of the world's largest and most reliable sources of comparable statistical, economic and social data. OECD databases span areas as diverse as national accounts, economic indicators, the labor force, trade, employment, migration, education, energy, health, industry, taxation, tourism and the environment Non-members are invited to subscribe to OECD agreements and treaties, and the Organization shares expertise and exchanges views on topics of mutual concern with more than 100 countries worldwide, from Brazil, China and Russia to least developed countries in Africa The OECD grew out of the Organization for European Economic Cooperation (OEEC), which was set up in 1947 with support from the United States and Canada to coordinate the Marshall Plan for the reconstruction of Europe after World War II. Created as an economic counterpart to NATO, the OECD took over from the OEEC in 1961 and, since then, its mission has been to help governments achieve sustainable economic growth and employment and rising standards of living in member countries while maintaining financial stability, so contributing to the development of the world economy.

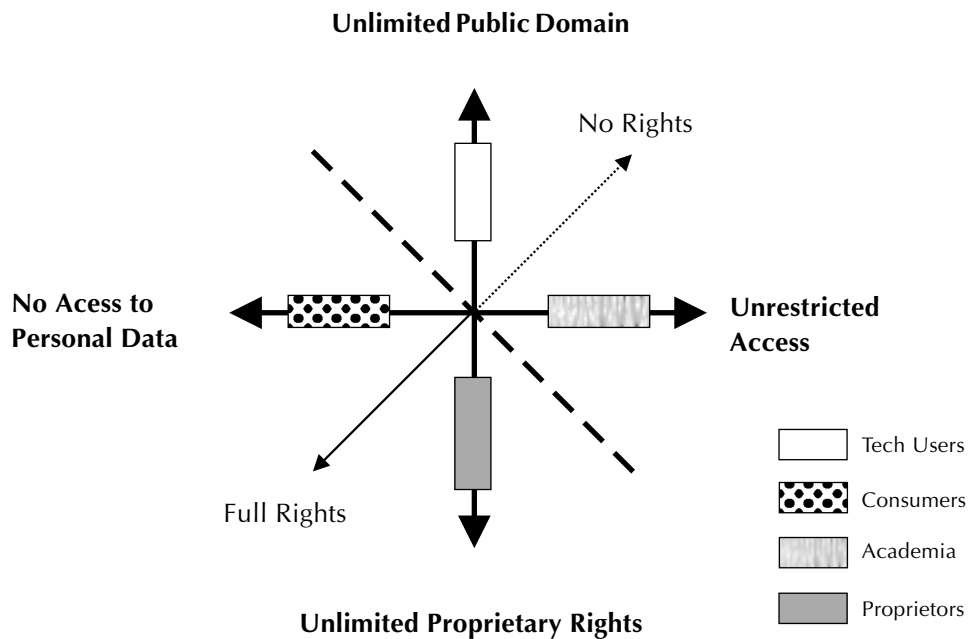
The Organization for Economic Cooperation and Development (2005), at www.oecd.org/about.

3 “Information and Communications Technologies, OECD Information Technology Outlook 2004: Highlights”, 2004 *Sci. & Info. Tech.* 15 (December 2004).

4 “The New Economy: Beyond Hype — The OECD Growth Project”, 2001 *Gen. Econ. & Future Stud.* 9, at pp. 41 and 42 (July 2001).

These guidelines establish minimum standards for the protection of privacy and individual liberties with respect to personal data and aim to reduce the differences among domestic rules and practices of countries. These standards also promote the economic interests of countries by encouraging data flows while preventing undue interference with such flows from personal data protection schemes.⁵

Figure 1. Balancing Proprietary and Privacy Rights: Who Can Claim a Right?



As demonstrated by Figure 1, above, this chapter will address two dimensions of conflicting interests in the world of dataflows: interests in proprietary rights, shown by the north-south continuum; and privacy interests, shown by the east-west continuum. The dotted line reflects the line of demarcation between the extremes of full rights in data (found in the region below the diagonal), and no rights in data (found in the region above the diagonal), whether those rights are proprietary in nature or pertain to privacy.

For purposes of this illustration, four basic constituencies can be identified, although no group reflects a simple, pure interest. The easiest constituency to identify is the proprietors of technology, as intellectual property rights holders, who are shown as the fully shaded box on the south-pointing ray. Their

⁵ Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 435.

interest is in having unlimited proprietary rights. Another easy group to identify is consumers, who are shown as the dotted white box on the west-pointing ray. Their interest is in having maximum protection for their personal data.

The third group consists of users (and not proprietors) of technology, shown as the white box on the north-pointing ray. They flourish in an unlimited public domain, as they have no claim to or desire to encounter vested interests in rights in the technology they use. The final group, academia, is shown as the box with stripes on the east-pointing ray. They are best served if they have unfettered access to information and technology to further their academic pursuits.

Typically, intellectual property rights holders have invested significant resources in collecting information that they then store in electronic databases. The information must achieve some measure of protection to return value to the intellectual property rights holder; otherwise, presumably, the intellectual property rights holder would not expend the resources necessary to collect and house the information. To protect and retain the value of the information collected, the intellectual property rights holder looks for tools, both legal and technological, to limit access to and use of the information he collects.

Generally, the law will grant exclusive rights to the intellectual property rights holder if he has created something novel, original, non-obvious, and useful.⁶ For example, a patent is an exclusive right that creates a temporary “monopoly” that allows the patent holder to set the market price of the invention and to control its sales.⁷

(b) Conflicting Interests

The intellectual property rights holder’s decision to innovate is dictated in large measure by the possible protection it can obtain for the innovation.⁸ Conversely, from the perspective of the academic, if the ability to exclude others or the control over the information is excessive, the sharing of information is then threatened, thereby inhibiting scientific progress, innovation, and growth.⁹

6 Report of the Department of Justice’s Task Force on Intellectual Property, United States Department of Justice, Office of the Attorney General, at p. 1 (October 2004).

7 “Patents and Innovation: Trends and Policy Challenges”, 2004 *Sci. & Info. Tech.* 4, at p. 9 (2004).

8 “The New Economy: Beyond Hype — The OECD Growth Project”, 2001 *Gen. Econ. & Future Stud.* 9, at p. 43 (July 2001).

9 “The New Economy: Beyond Hype — The OECD Growth Project”, 2001 *Gen. Econ. & Future Stud.* 9, at p. 44 (July 2001).

With respect to the consumer, or the individual, the Privacy Commissioner for British Columbia, Canada, has identified four tensions created by trends in data flows, namely:

1. Partly because there is no international consensus on the fundamental principles on which the protection of the individual should be based,¹⁰ technology's impact on data management has driven public policy on privacy when, arguably, public policy should drive the data management methods employed.
2. Without consistent privacy regimes, regulating the use of personal information once it crosses borders is virtually impossible.
3. As the world's reliance on digitally stored, analyzed, and accessed personal information increases, so does the risk that the information is inaccurate, that the information will be used out of context, or that the information will simply be misused, whether intentionally or not.
4. The distinction between commercial and government uses of personal information is becoming blurred and will increase the risks to privacy and to other individual rights and interests.¹¹

However, when information is viewed at a macro or collective level, and not as individual records, concerns for personal privacy may give way to other concerns about affording collectors of information a reward for the sweat of their brow and encouraging the free flow of information for the betterment of society. These social forces are the underpinnings of intellectual property rights — the *quid pro quo*. Rights in intellectual property should strike a balance between ensuring sufficient private returns on investment in innovations in exchange for the disclosure and diffusion of those new inventions.¹²

Through this exchange, human endeavor flourishes. Innovators are inspired by new ideas or artistic visions, and those inspirations lead to the creation of new works, such as books and music, or inventions for the nation's benefit.¹³

Yet, if there is unequal access to new technology or the tools to learn how to use technology effectively, this exchange is no longer what society has

10 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 430 (1981).

11 Report on the Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, at p. 14, (October 2004).

12 "The New Economy: Beyond Hype — The OECD Growth Project", 2001 *Gen. Econ. & Future Stud.* 9, at p. 43 (July 2001).

13 Report of the Department of Justice's Task Force on Intellectual Property, United States Department of Justice, Office of the Attorney General, at p. 1 (October 2004).

bargained for. Such inequality has become a matter of major policy concern because a knowledge and technology divide could lead to whole segments of society becoming less and less capable of participating in the economy.¹⁴

Additionally, disparities in national legislation could hamper the flow of personal data across borders. Restrictions on these information flows could cause serious disruption in important sectors of the economy, such as banking and insurance. Data flows in these industries have greatly increased in recent years, and further increase is anticipated due to the widespread introduction of new computer and communications technologies.¹⁵ At the governmental level, countries have a common interest in policy harmonization to prevent the creation of locations where national regulations on data processing can be circumvented easily.¹⁶ Without harmonization, transborder data flows will confront inconsistent barriers, creating technological vacuums.

When societies and cultures are open and subject to the free flow of data, the markets available to innovators and consumers increase, as does diffusion of knowledge, technologies, and new business practices. Furthermore, the international mobility of people and goods in commerce reinforces the need for consistent practices with regard to the processing of personal data.¹⁷

This is especially true in light of the advent of the Internet. Globally, the Internet supports critical infrastructures such as energy, transportation, and finance and causes the world to be interconnected by allowing information to flow easily across national borders.¹⁸ Harmonization of the opposing interests of intellectual property rights and the public domain, personal privacy, and the free flow of data requires a balance of the elements shown in Figure 1 and described above, whereby harmonization becomes greatest at the center point.

14 “The New Economy: Beyond Hype — The OECD Growth Project”, 2001 *Gen. Econ. & Future Stud.* 9, at p. 67 (July 2001).

15 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 427 (1981).

16 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 431 (1981).

17 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 431 (1981).

18 “Organization for Economic Cooperation and Development, Guidelines for the Security of Information Systems and Networks”, 2002 *Sci. & Info. Tech.* 9 at p. 7 (2002).

2.02 Framework for Discussion

(a) In General

Data is generally defined as representations of information or concepts in any form.¹⁹ A subset of data is personal data, which refers to any information relating to an identified or identifiable individual.²⁰

The transmission or movement of personal data across national borders is referred to as transborder flows of personal data.²¹ Laws that regulate transborder flows of personal data are known as data protection, or privacy protection, laws.²²

The flow of data and the subsequent analysis of that data are critical to the information and communication technology sector, which plays a pivotal role in the world economy.²³ The information and communication technology sector comprises manufacturing and services industries that capture, transmit, and display data and information electronically and is the portion of the global economy that best measures the use of data and transborder data flows.²⁴

(b) Data Mining

One type of analysis that is performed on data is called “data mining”. Data mining is:

. . . the application of database technology and techniques to uncover patterns and relationships in data and to undertake the prediction of future results or behavior.²⁵

-
- 19 Personal Information Protection and Electronic Documents Act, ch. 5, S.C. 31 (1) (2000) (Can.).
- 20 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 423 (1981).
- 21 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 423 (1981).
- 22 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at pp. 422 and 424 (1981).
- 23 “The New Economy: Beyond Hype — The OECD Growth Project”, 2001 *Gen. Econ. & Future Stud.* 9, at p. 3 (July 2001).
- 24 “Measuring the Information Economy 2002: The ICT Sector”, 2002 *Sci. & Info. Tech.* 14, at p. 81 (2002). Gray *et. al.*, “Memorandum on the Legal Need for H.R. 3261, the Database and Collections of Information Misappropriation Act”, 21 No. 5 *Comp. & Internet L.* 2 (2004).
- 25 Report on the Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, at p. 14 (October 2004).

The “raw” data that is collected and any subsequent data generated through processing techniques, such as data mining, are then stored in data banks.

Indeed, data mining can be used to:

. . . discover previously unknown facts and phenomena about a database, answering questions users did not know to ask. They carry out the analysis without receiving a hypothesis from the human analyst, instead searching for hidden patterns on their own . . . mak[ing] predictions about future data.²⁶

Data banks are collections of data intended for retrieval and other purposes.²⁷ In non-technical terms, a database connotes any electronic compilation of data that is organized and indexed in a way that allows users to access, retrieve, and query data efficiently.²⁸ While the compilation and production of information contained in databases is expensive, the electronic form of the data coupled with digital technology make it cheap to copy.²⁹ Furthermore, despite the expense associated with compiling data, data alone does not qualify for legal protection through intellectual property rights regimes.

(c) Proprietary and Privacy Rights

The recognition of data in intellectual property rights schemes fuels debates on the essence of proprietary rights. The achievement of intellectual property rights status requires that certain conditions be met or bargains struck — the *quid pro quo*. Of all intellectual property rights, the ones considered most potent are those granted to holders of patents. Patents are granted for an invention that is novel, non-obvious, and industrially applicable and are awarded to:

. . . [w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof³⁰

Patents promote the useful art and, as such, cannot be granted for some types of newly discovered substances, theories, abstract ideas, or laws of nature because doing so takes away from the public body of knowledge and would

26 Zarsky, “Mine Your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion”, 5 *Yale L.J.* 4 (2002).

27 Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 *I.L.M.* 422, at p. 430 (1981).

28 Greenbaum, “The Database Debate: In Support of an Inequitable Solution”, 13 *Alb. L.J. S.C.I & Tech.* 431, at p. 441 (2003).

29 Gibson, “Re-Reifying Data”, 80 *Notre Dame L. Rev.* 163, at p. 164 (2004).

30 35 United States Code, section 101.

unnecessarily grant a patent holder the right to constrict the flow of information. Once granted, the patent holder has the legal authority to exclude others from commercially exploiting the invention for the limited period of time of the grant, generally 20 years.³¹

In return for the legal authority to exclude others, the patent holder must disclose information relating to the invention for which protection is granted. The patent holder's disclosure of the invention's details in exchange for a grant of legal authority is thus an important aspect of the patenting system *quid pro quo*.³²

This exchange both encourages the development of inventions and the practical application of those inventions by making the invention available to the rest of the industry and the general public from which to learn. The diffusion of inventions under this type legal framework leads to greater innovation that ultimately impacts and increases economic performance on a national scale.³³

A similar framework exists for copyrights, another form of intellectual property rights. As with patents, copyrights make an author's work exclusive, which provides an incentive to incur the costs of producing or creating the work, so long as these costs are less than or equal to the value that consumers, or the marketplace, put on the work.³⁴

However, data and facts are the building blocks for subsequent inventions or works and are too useful to restrict access to them through property rights.³⁵ From the perspective of the public domain, facts are valuable components of future works and should be available and free for all to use.³⁶ As summarized by the United States Supreme Court:

... [t]he economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors in science and useful art.³⁷

Under this philosophy, databases are copyrightable in the United States as compilations of information that consist of data that have been processed

31 Schwartz, *Patent Law and Practice* (4th ed., 2003), at p. 65.

32 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, at p. 7 (2004).

33 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, at p. 7 (2004).

34 Green, "Copyrighting Facts", 78 *Ind. L.J.* 919, at p. 925 (2003).

35 Green, "Copyrighting Facts", 78 *Ind. L.J.* 919, at p. 921 (2003).

36 Green, "Copyrighting Facts", 78 *Ind. L.J.* 919, at p. 922 (2003).

37 *Mazer v. Stein*, 347 U.S. 201, at p. 219 (1954).

along with the original data elements, or pre-existing information that was collected.³⁸ To qualify for copyright protection, the work must demonstrate originality and creative authorship as prerequisites to copyright protection, as opposed to depending on the industrious effort, i.e., sweat of the brow, or commercial value standards.³⁹ Therefore, copyright protection does not extend to facts or ideas, regardless of the effort or expense incurred in obtaining them.⁴⁰ Derived from this concept is “one of the most pervasive and oft-cited principles in copyright law” — copyright protects the expression of an idea, but not the idea itself.⁴¹ The level of proprietary rights in data, therefore, is dependent on the amount and type of processing that is done to the data after it is collected.

A slightly different philosophy has been implemented in Europe. There, European Union (EU) Directives have established a database right that is measured in terms “of its own kind”, or *sui generis*, and not by the creative additions made by the author. This database right is determined by the level of investment in the database and is designed to protect the investment from those who wish to take advantage of its value, whether the information itself, its accuracy, or its completeness, without compensating the database owner.⁴²

An effective adjunct to these rights is the notion of trade secrecy, whereby the maintenance of the secret nature of information affords the holder a real or potential economic advantage. Rights of trade secret holders against misappropriation is a fundamental intellectual property right in the world of data collectors and databases and an alternative to the *quid pro quo* of patent and copyright rights, so long as the confidentiality of the information remains intact.

Although the assumption from an intellectual property rights perspective is that data, without more, does not satisfy the requirements necessary for a patent, copyright, *sui generis* right, or trade secret protection and is freely

38 Leaffer, *Understanding Copyright Law* (3d ed., 1999), at pp. 68 and 73. 17 United States Code, section 101 (“A compilation is a work formed by the collection and assembling of pre-existing materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship”).

39 Leaffer, *Understanding Copyright Law* (3d ed., 1999), at pp. 56 and 64, citing *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991). 17 United States Code, section 102 (“[c]opyright protection subsists . . . in original works of authorship”).

40 17 United States Code, section 102(b) (“In no case does copyright protection for an original work of authorship extend to any idea . . .”).

41 Leaffer, *Understanding Copyright Law* (3d ed., 1999), at p. 77.

42 Stephens, “Database Rights: A Surprise Judgment by the European Court of Justice”, 18 *World Intell. Prop. Rep.* 12 (1 December 2004).

available to all; however, from a privacy rights perspective, those about whom the data pertain may nonetheless prohibit the free distribution and access to data containing personal information. Indeed, the amount of processing done to data raises concerns about the impact of information technology on privacy.⁴³ One such concern is that:

The hidden patterns and subtle relationships that data mining detects are recorded and become personal information about the individual whose characteristics or habits are being searched and analyzed.⁴⁴

While the right to privacy is not absolute, the increased international flow of personal information from both the private and the public sectors has triggered nations to reevaluate privacy protections. As early as the 1970s, European countries began enacting the first privacy laws in response to the increased collection, processing, and subsequent transborder flow of data.⁴⁵ These laws have now seen their maturation in the EU Data Protection Directive and similar laws, such as the Personal Information Protection and Electronic Documents Act of Canada.

(d) The Expanding Market for Information

Concurrently, advances in technology and trade liberalization have increased the market for information products and services.⁴⁶ For example, data-management companies compete to offer technology and services for storing, organizing, and accessing information.

Governments are following the lead of corporations and are contracting out data processing and other data services formerly done in-house.⁴⁷ This leads inexorably back to the axes of Figure 1 — the goal of harmonization is to tame the tensions of antipodal interests through the intellectual property rights *quid pro quo* and to balance the personal right to privacy with the gains to be derived from data compilations and analysis.

43 Report on Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, at p. 12 (October 2004).

44 Report on Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, at p. 14 (October 2004).

45 Report on Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, at p. 13 (October 2004).

46 Lipton, “Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases”, 18 *Berkeley Tech. L.J.* 773, at pp. 779–783 (2003).

47 Report on Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia at pp. 12 and 13 (October 2004).

2.03 The Value of Data

(a) In General

Data has tremendous value, as reflected in the wide range of information products it has spawned. Examples of information products based on personal data include statistics on consumer spending habits and health, insurance, or financial status. Other products are based on factual data, such as scientific, technological, or educational information. Often databases derive their value directly from the commercial value of the business, such as when they form the core of a company's business operations, as they do in travel planning, stock brokering, and online shopping.⁴⁸

Additionally, if the database qualifies for legal protection under intellectual property rights regimes, the database is transformed from an intangible electronic asset into an exclusive property right with independent market value because it can be licensed, mortgaged, or leveraged to obtain financing for other business ventures.⁴⁹

Physical assets no longer necessarily represent the bulk of the value of a company. "Increasingly, and largely as a result of the information technologies revolution and the growth of the service economy, companies are realizing that intangible assets are often becoming more valuable than their physical assets."⁵⁰ Now, the development and application of intellectual property rights are "the keys to greater competitiveness in fiercely competitive markets."⁵¹

With respect to markets for information products, there are other competitive forces at play. The data contained within the information products and in databases are a mixture of public and private interests, as demonstrated by Figure 1. Those who seek to exploit the databases commercially value the private property rights in databases. Those whose consumer spending habits are contained in the database value their individual privacy above the intellectual property rights holder's right to exploit the database, while those in academia who seek answers and explanations to life's mysteries value the data for its research and teaching potential.⁵²

48 Lipton, "Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases", 18 *Berkeley Tech. L.J.* 773, at p. 775 (2003).

49 *Intellectual Property for Business*, World Intellectual Property Organization, Small and Medium-Sized Enterprises Division, at pp. 6 and 15 (2005).

50 *Intellectual Property for Business*, World Intellectual Property Organization, Small and Medium-Sized Enterprises Division, at p. 5 (2005).

51 *Intellectual Property for Business*, World Intellectual Property Organization, Small and Medium-Sized Enterprises Division, at p. 5 (2005).

52 Lipton, "Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases", 18 *Berkeley Tech. L.J.* 773, at pp. 779 and 780 (2003).

(b) Impact of the Internet on Value

The World Intellectual Property Organization (WIPO) predicted that, since most literary and artistic works can be digitized or are created digitally, the Internet would be the logical way to access them.⁵³

The WIPO further predicted that the Internet would become an immense library of all existing works where creators worldwide would have available, at their discretion, the building blocks to create new works. In building new works, authors then simply revise and combine existing works in new ways.⁵⁴ This is the “big bang” theory of cyberspace, where masses of digital works swirling over electronic networks become the breeding ground for explosions in global intellect.

(c) Sales of Intellectual Property Rights

Another way to value data is by sales of intellectual property rights. In 2002, United States copyright industries accounted for an estimated six per cent of the nation’s Gross Domestic Product, or US \$626.6-billion), and sold and exported US \$89.3-billion to foreign nations.⁵⁵

Additionally, in the fourth quarter of 2002 alone, the United States had more than US \$14-billion in retail e-commerce⁵⁶ sales, which was more than 1.6 per cent of retail sales.⁵⁷ E-commerce and the sale of intellectual property rights are considered part of the information and communication technology sector.⁵⁸

In general, firms have benefited from increased productivity resulting from the use of information and communication technology. Recent surveys show that 24 per cent of businesses in Japan use information and communication technology, followed by 20 per cent in Canada, 17 per cent in the United

53 Electronic Commerce and Copyright: A Key Role for WIPO, World Intellectual Property Organization, Advisory Committee on Management of Copyright and Related Rights in Global Information Networks, at section II(1) (1999).

54 Electronic Commerce and Copyright: A Key Role for WIPO, World Intellectual Property Organization, Advisory Committee on Management of Copyright and Related Rights in Global Information Networks, at section II(1) (1999).

55 Report of the Department of Justice’s Task Force on Intellectual Property, United States Department of Justice, Office of the Attorney General, at p. 7 (October 2004).

56 “Measuring the Information Economy 2002: The ICT Sector”, 2002 *Sci. & Info. Tech.* 14, at p. 89 (2002) (e-commerce is narrowly defined as an Internet transaction that consists of the sale or purchase of goods or services between any two entities conducted over the Internet, though the payment and ultimate delivery of the good or service may be conducted off-line).

57 Seizing the Benefits of ICT in a Digital Economy, Meeting of the OECD Council at Ministerial Level, at p. 6, fig. 1 (2003).

58 “Measuring the Information Economy 2002: The ICT Sector”, 2002 *Sci. & Info. Tech.* 14, at pp. 81 and 82 (2002).

States and Korea, and 14 per cent in Germany and Ireland.⁵⁹ In this sector, scientific and technological advances have resulted from waves of innovation that are centered less on individual firms and more on global networks of information products and databanks.⁶⁰

(d) Value through Grants of Intellectual Property Rights

Another means to value data from the perspective of the government is by measuring the number of intellectual property rights grants made. A primary measure of innovation and technology output are patents, because they presumably reflect inventive performance. Since part of the intellectual property rights grant includes disclosure of information about the patent, patents also indicate the level of diffusion of knowledge across technology areas and countries.⁶¹ Worldwide, the total number of patents has grown by more than four per cent per year since 1985, with 44,000 patents with a priority date in 2000.⁶²

The number of patents takes into account filings in different countries for substantially the same claims.⁶³ The priority date is the date closest to the date of invention.⁶⁴ Using the priority date removes the bias that the application or grant dates introduce, which are associated with administrative delay and a prosecution strategy, neither of which reflect technology output.⁶⁵

In addition, there is a time lag between the priority date and the availability of the application or grant information.⁶⁶ In 2002, more than 850,000 patent applications were filed in Europe, Japan, and the United States, up from approximately 600,000 in 1992. Between 1992 and 2002, the number of patent applications filed in Europe, Japan, and the United States increased by more than 40 per cent.⁶⁷

59 ICT Access Now, Widespread but Laggard Users Risk New Digital Divide, Warns OECD, Seizing the Benefits of Information and Communication Technology in a Digital Economy, Meeting of the OECD Council at Ministerial Level, at p. 6, fig.1 (14 December 2004).

60 "Patents and Innovation: Trends and Policy Challenges", 2004 *Sci. & Info. Tech.* 4, at p. 5 (2004).

61 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, at p. 7 (2004).

62 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, at p. 14 (2004).

63 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, p. 11 (2004).

64 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, p. 40 (2004).

65 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, p. 10 (2004).

66 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, p. 40 (2004).

67 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, p. 5 (2004).

(e) Commercial Value of Collection and Use of Data

“The collection and sale of information is an industry worth many billions of dollars a year to American companies and is a primary engine of economic growth.”⁶⁸ Economic growth in the information and communication technology sector on correlates with increased collection of and uses of personal data. Innovation has become increasingly a collaborative, global process involving a larger number of more diverse actors, primarily involving multinational enterprises.⁶⁹ Furthermore, the expansion of information and communication technology and the Internet has accelerated the availability of information and facilitated the globalization of innovation. Businesses, governments, consumers, and key infrastructures increasingly rely on the use of information and communication technology, which are often interconnected at the global level.⁷⁰

The commercial value of personal data, therefore, tracks the value of data in general. Indeed, it may be more valuable, because the data information and communication technology users encounter are guaranteed to contain and rely on personal data. Not surprisingly, as e-commerce transactions have increased, so have consumer complaints regarding security and privacy protection.⁷¹

Databases and databanks that house all of the data collected and created from transactions and data mining are prone to full-scale misappropriation because the information contained within them is highly vulnerable, in its electronic form, as “[i]nformation, by its very nature, is ubiquitous, inexhaustible, and indivisible.”⁷²

The digital format of data adds value to the data because computers can then process data on a massive scale, thereby vastly expanding the possibilities of storing, comparing, linking, selecting, and accessing personal data through the combination of computers and telecommunications technologies while facilitating misappropriation. Not surprisingly, then, unauthorized copying of databases has already reached significant levels.⁷³

68 Green, “Copyrighting Facts”, 78 *Ind. L.J.* 919, at p. 923 (2003).

69 *Organization for Economic Cooperation and Development, Compendium of Patent Statistics* (2004), at <http://www.oecd.org/dataoecd/60/24/8208325.pdf>, p. 15 (2004).

70 *Seizing the Benefits of ICT in a Digital Economy*, Meeting of the OECD Council at Ministerial Level, at p. 18 (2003).

71 *Seizing the Benefits of ICT in a Digital Economy*, Meeting of the OECD Council at Ministerial Level, at p. 20 (2003).

72 Grosheide, “Database Protection — The European Way”, 8 *Wash. U. J.L. & Pol’y* 39, at p. 40 (2002).

73 Green, “Copyrighting Facts”, 78 *Ind. L.J.* 919, at p. 923 (2003).

In addition to potentially violating any number of laws, misappropriation leads to public disclosure of the information, after which the information can potentially be used without any obligation to the original intellectual property rights' holder.⁷⁴

Misappropriation of intellectual property rights impacts society in two ways. First, intellectual property theft alters the economic equilibrium of markets and undermines competition. Second, intellectual property theft can impact the health, safety and financial well-being of individuals, for example, through counterfeit products and identify theft.⁷⁵

(f) Counterfeiting

It is estimated that counterfeiting accounts for five per cent to seven per cent of global merchandise trade, equivalent to US \$512-billion in lost sales.⁷⁶ Worldwide, intellectual property theft is estimated to cost American companies alone US \$250-billion a year.⁷⁷

As a direct result of counterfeit products and Internet theft of intellectual property, governments and the economy suffer, for example, from the loss of hundreds of millions of dollars in tax revenues, wages, and investment dollars, not to mention hundreds of thousands of jobs.⁷⁸

(g) Identity Theft

Another risk of the dissemination of personal data in a digital format over the Internet is identity theft. In the United States, identity fraud costs consumers more than US \$50-billion.

It is estimated that there are more than 9-million new identity theft victims per year at a cost of more than US \$5,500 per victim, who spend on average 28 hours resolving the problems caused by the fraud.⁷⁹

74 Grosheide, "Database Protection —The European Way", 8 *Wash. U. J.L. & Pol'y* 39, at p. 40 (2002).

75 Report of the Department of Justice's Task Force on Intellectual Property, United States Department of Justice, Office of the Attorney General, at p. 7 (October 2004). The report also explains that intellectual property theft has been linked to organized crime and possibly funds terrorism.

76 Balfour, "FAKES! The Global Counterfeit Business is Out of Control, Targeting Everything from Computer Chips to Life-saving Medicines. It's so Bad That Even China May Need to Crack Down", *Business Week*, at p. 56 (2005).

77 Report of the Department of Justice's Task Force on Intellectual Property, United States Department of Justice, Office of the Attorney General, at p. 8 (October 2004).

78 Report of the Department of Justice's Task Force on Intellectual Property, United States Department of Justice, Office of the Attorney General, at p. 8 (October 2004).

79 *Identity Fraud Survey Report 2005*, Better Business Bureau, at p. 3 (2005).

(h) Enforcement

There is a general concern that, because intellectual property crime is lucrative and has immense profit margins, current enforcement methods are inadequate to combat it.⁸⁰

In the face of a dearth of statutory or judicially created property rights in raw data and inconsistent regimes to enforce what rights there are, the value of data has led data collectors to use contracts and technological protections to control information for commercial exploitation.⁸¹

Risk of theft and misuse is mitigated when there are fair and clear standards for enforcement of laws that protect the various rights and when enforcement efforts are effective and not arbitrary. On a global scale, this requires harmonization. The EU has recognized that “to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent” wherever the data goes.⁸²

Furthermore, harmonization is vital to the market economy, “especially in view of the scale of the divergences which currently exist between the relevant laws”.⁸³ As such, there needs to be global coordination of the laws “to ensure that the cross-border flow of personal data is regulated in a consistent manner”.⁸⁴

2.04 Legal Factors in Protecting Intellectual Property

(a) In General

Intellectual property rights, including patents, copyrights, trade secrets, and trade marks, provide a panoply of tools to protect intellectual property, in general, each variety with its own unique qualities, characteristics, and limitations.

80 Report of the Department of Justice’s Task Force on Intellectual Property, United States Department of Justice, Office of the Attorney General, at p. 9 (October 2004).

81 Lipton, “Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases”, 18 *Berkeley Tech. L.J.* 773, at p. 781 (2003).

82 Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995, *O.J.* (L 281/31) 8.

83 Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995, *O.J.* (L 281/31) 8.

84 Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995, *O.J.* (L 281/31) 8.

The world has seen substantial efforts to harmonize the national treatment of intellectual property rights. In fact, harmonization efforts, in the form of treaties and international agreements, reflect an integral part of the intellectual property rights landscape. Some of the more renowned treaties are discussed below.

(b) Berne Convention

The Berne Convention is the oldest international treaty in the field of copyright, boasting 159 signatories.⁸⁵ It aims “to protect, in as effective and uniform a manner as possible the rights of authors in their literary and artistic works”,⁸⁶ and provides for national treatment, such that works originating in one of the member states are to be given the same protection in each of the member states as those granted to works of their own nationals.⁸⁷

The Berne Convention protects authors of works,⁸⁸ which include any original production in the literary, scientific and artistic domain, or derivative

85 The Contracting Parties are: Albania, Algeria, Andorra, Antigua and Barbuda, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belarus, Belgium, Belize, Benin, Bhutan, Bolivia, Bosnia and Herzegovina, Botswana, Brazil, Bulgaria, Burkina Faso, Cameroon, Canada, Cape Verde, Central African Republic, Chad, Chile, China, Colombia, Comoros, Congo, Costa Rica, Croatia, Cuba, Cyprus, Czech Republic, Côte d’Ivoire, Democratic People’s Republic of Korea, Democratic Republic of the Congo, Denmark, Djibouti, Dominica, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Estonia, Fiji, Finland, France, Gabon, Gambia, Georgia, Germany, Ghana, Greece, Grenada, Guatemala, Guinea, Guinea-Bissau, Guyana, Haiti, Holy See, Honduras, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Latvia, Lebanon, Lesotho, Liberia, Libyan Arab Jamahiriya, Liechtenstein, Lithuania, Luxembourg, Madagascar, Malawi, Malaysia, Mali, Malta, Mauritania, Mauritius, Mexico, Micronesia (Federated States of), Monaco, Mongolia, Morocco, Namibia, The Netherlands, New Zealand, Nicaragua, Niger, Nigeria, Norway, Oman, Pakistan, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Republic of Korea, Republic of Moldova, Romania, Russian Federation, Rwanda, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Saudi Arabia, Senegal, Serbia and Montenegro, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sudan, Suriname, Swaziland, Sweden, Switzerland, Syrian Arab Republic, Tajikistan, Thailand, The Former Yugoslav Republic of Macedonia, Togo, Tonga, Trinidad and Tobago, Tunisia, Turkey, Ukraine, United Arab Emirates, United Kingdom, United Republic of Tanzania, United States, Uruguay, Uzbekistan, Venezuela, Viet Nam, Zambia, and Zimbabwe. The World Intellectual Property Organization (2005), at http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15.

86 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 262 (quoting Berne Convention preamble).

87 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 262.

88 Berne Convention, article 3.

works, which are based on other, pre-existing works, such as translations, adaptations, arrangements, or alterations of a literary or artistic work.⁸⁹ The Berne Convention establishes minimum standards of protection for the works of authors and the minimum duration of such protection.⁹⁰ For example, authors are granted the exclusive right of reproduction in any manner or form and the exclusive right to make adaptations, arrangements, or other alterations of the author's work.⁹¹

In keeping with its philosophical underpinnings of *quid pro quo*, the Berne Convention also provides limitations on the author's exclusive rights. These exceptions allow for the use of a work, without the owner's authorization and without obligation to pay the owner for the use.⁹² Examples of such uses are called "free use" of protected works and include use by way of illustration or teaching purposes and use for the purpose of reporting current events.⁹³ Examples from the United States are:

1. Necessary copies that are required for operation of a program or a back-up copy;⁹⁴
2. The "first sale doctrine;"⁹⁵ and
3. The "fair use" doctrine.⁹⁶

These statutory exceptions are designed to keep the balance between the intellectual property rights holder's exclusive rights and the furtherance of the art.

While the Berne Convention was revised regularly to respond to new technological developments, new treaties were needed as the international norms of the Berne Convention failed to provide adequate guidance for the challenges of new technologies.⁹⁷ Under article 20 of the Berne Convention, the countries of the Union may "enter into special agreements among themselves, in so far as such agreements grant to authors more extensive rights than those granted by the

89 Berne Convention, article 2.

90 "International Treaties and Conventions on Intellectual Property", *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 263.

91 Berne Convention, articles 9 and 12.

92 "International Treaties and Conventions on Intellectual Property", *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 264.

93 Berne Convention, articles 10 and 10 *bis*.

94 17 United States Code, section 117(a).

95 17 United States Code, section 109.

96 17 United States Code, section 107.

97 "International Treaties and Conventions on Intellectual Property", *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 269.

Convention, or contain other provisions not contrary to th[e] Convention”.⁹⁸ Through this provision, the WIPO Copyright Treaty of 1996 was created.⁹⁹

(c) World Intellectual Property Organization Copyright Treaty

The WIPO Copyright Treaty applies to computer programs and compilations of data or other material, such as databases, in any form, for which by reason of the selection or arrangement of their contents constitute intellectual creations.¹⁰⁰ In fact, the WIPO Copyright Treaty has “established the new international legal norms for [the] protection of technological measures”.¹⁰¹ Entering into force on 6 March 2002, the WIPO Copyright Treaty is now in force in 51 countries, with more than 20 more signatories.¹⁰² The Director General of WIPO is the depositary of the WIPO Copyright Treaty.¹⁰³

The Treaty addresses:

... the need to introduce new international rules and clarify the interpretation of certain existing rules to provide adequate solutions to the questions raised by new economic, social, cultural and technological developments¹⁰⁴

It also recognizes:

... the profound impact of the development and convergence of information and communication technologies on the creation and use of literary and artistic works¹⁰⁵

98 Berne Convention, article 20.

99 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 269.

100 World Intellectual Property Organization Copyright Treaty, articles 4 and 5.

101 Current Developments in the Field of Digital Rights Management, World Intellectual Property Organization Standing Committee on Copyright and Related Rights, 1 August 2003, S.C.C.R./10/2, at p. 41.

102 The Contracting Parties are Argentina, Armenia, Austria, Belarus, Belgium, Bolivia, Botswana, Bulgaria, Burkina Faso, Canada, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Ecuador, El Salvador, Estonia, European Communities, Finland, France, Gabon, Georgia, Germany, Ghana, Greece, Guatemala, Guinea, Honduras, Hungary, Indonesia, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Mali, Mexico, Monaco, Mongolia, Namibia, The Netherlands, Nicaragua, Nigeria, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Saint Lucia, Senegal, Serbia and Montenegro, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Togo, Ukraine, United Arab Emirates, United Kingdom, United States, and Uruguay. WIPO Copyright Treaty, article 20. World Intellectual Property Organization (2005), at http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16.

103 World Intellectual Property Organization Copyright Treaty, article 25.

104 World Intellectual Property Organization Copyright Treaty, Preamble.

105 World Intellectual Property Organization Copyright Treaty, Preamble.

Furthermore, the WIPO Copyright Treaty aims to:

... maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention.¹⁰⁶

Article 11 of the WIPO Copyright Treaty obliges its signatories, or “contracting parties”, to provide legal remedies against the circumvention of technological measures used by authors in connection with the exercise of their rights and against the removal or altering of information, such as certain data that identify works or their authors, which are necessary for the management and distribution of their intellectual property rights.¹⁰⁷ The WIPO Copyright Treaty obliges each contracting party to adopt, in accordance with its legal system, the measures necessary to ensure the application of the WIPO Copyright Treaty.

In particular, the contracting party must ensure that enforcement procedures are available under its law so as to permit effective action against any act of infringement of rights covered by the WIPO Copyright Treaty.¹⁰⁸ Such action must include expeditious remedies to prevent infringement and remedies, which will constitute an effective deterrent to further infringements.¹⁰⁹

Despite these enhanced enforcement provisions, the WIPO Copyright Treaty remains true to the *quid pro quo* concept. Although it recognizes the “outstanding significance of copyright protection as an incentive for literary and artistic creation”,¹¹⁰ it reaffirms the limits of copyright protection “to expressions and not to ideas, procedures, methods of operation, or mathematical concepts”, or raw data.¹¹¹

Furthermore, the WIPO Copyright Treaty allows contracting parties to provide for limitation of or exceptions to the rights granted to authors of literary and artistic works under the treaty in certain special cases that do not conflict with the normal exploitation of the work.¹¹² These limitations, in conjunction with the limiting language of article 11 of the Treaty, enable the Contracting Parties to allow for exceptions such as fair use by not allowing an author to exercise rights that are beyond those granted by the Berne Convention.¹¹³

106 World Intellectual Property Organization Copyright Treaty, Preamble.

107 World Intellectual Property Organization Copyright Treaty, article 11.

108 World Intellectual Property Organization Copyright Treaty, article 12.

109 World Intellectual Property Organization Copyright Treaty, article 14.

110 World Intellectual Property Organization Copyright Treaty, Preamble.

111 World Intellectual Property Organization Copyright Treaty, article 2.

112 World Intellectual Property Organization Copyright Treaty, article 10.

113 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 42.

(d) Trade Related Aspects of Intellectual Property Rights Agreement

Another substantial step in intellectual property rights harmonization occurred when the Trade Related Aspects of Intellectual Property Rights Agreement (TRIPS) came into effect on 1 January 1995. To date, it is the most comprehensive multilateral agreement on intellectual property.¹¹⁴ The areas of intellectual property that it covers are:

1. Copyright and related rights (i.e., the rights of performers, producers of sound recordings, and broadcasting organizations);
2. Trade marks, including service marks;
3. Geographical indications, including appellations of origin;
4. Industrial designs;
5. Patents, including the protection of new varieties of plants;
6. Layout-designs of integrated circuits; and
7. Undisclosed information, including trade secrets and test data.¹¹⁵

Like the international treaties before it, TRIPS provides for national treatment.¹¹⁶ TRIPS sets out the minimum standards of protection and the duration of protection to be provided by each member state for the above areas of intellectual property. Furthermore, TRIPS establishes general principles that are applicable to all intellectual property rights enforcement procedures. As a minimum standards agreement, TRIPS allows member states to provide more extensive protection of intellectual property and to determine the appropriate method of implementation of the TRIPS' provisions within national law.¹¹⁷

Article 10 of TRIPS addresses computer programs and compilations of data. It “clarifies that databases and other compilations of data or other material shall be protected as such under copyright even where the databases include data that as such are not protected under copyright”.¹¹⁸ Specifically, article 10 states:

Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their

114 There are 148 members of the World Trade Organization.

115 World Trade Organization, at http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (2005).

116 Trade Related Aspects of Intellectual Property Rights Agreement, article 3. (“Each member shall accord to the nationals of other members treatment no less favorable than that it accords to its own national with regard to the protection of intellectual property”).

117 World Trade Organization, at http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (2005).

118 World Trade Organization, at http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (2005).

contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data itself, shall be without prejudice to any copyright subsisting in the data or material itself.¹¹⁹

TRIPS also provides enhanced protection against unfair competition by protecting undisclosed information, such as trade secrets and know-how, so long as that information is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret.¹²⁰

(e) Paris Convention

Another intellectual property treaty is the Paris Convention, which provides international protection of industrial property within the Union.¹²¹ Industrial property is one category of intellectual property “which includes inventions (patents), trademarks, industrial designs, and geographic indications of source”; the other category of intellectual property is copyright, “which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs”.¹²²

The Paris Convention guarantees the right to national treatment, the right of priority, establishes a number of common rules in the field of substantive law, and establishes the administrative framework to implement the Convention.¹²³ The industrial property covered by the Paris Convention includes:

1. Patents;
2. Utility models;
3. Industrial designs;
4. Trade marks;
5. Service marks;
6. Trade names; and
7. Indications of source or appellations of origin.¹²⁴

Moreover, the Paris Convention applies not only to industrial property used in commerce and industry, but also to agricultural and extractive industries

119 Trade Related Aspects of Intellectual Property Rights Agreement, article 10.

120 Trade Related Aspects of Intellectual Property Rights Agreement, article 39.

121 Paris Convention, article 1(1). (“The countries to which this Convention applies constitute a Union”).

122 World Intellectual Property Organization, at <http://www.wipo.int/about-ip/en/> (2005).

123 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 242.

124 Paris Convention, article 1(2).

and to all manufactured or natural products.¹²⁵ It establishes protection against direct or indirect use of a false indication of source of the goods or the identity of the producer, manufacturer, or merchant¹²⁶ and against any act of competition contrary to honest practices in industrial or commercial matters, or unfair competition.¹²⁷

Under the Paris Convention:

. . . [n]ationals of any country of the Union shall, as regards the protection of industrial property, enjoy in all the other countries of the Union the advantages that their respective laws now grant . . . to nationals; all without prejudice to the rights especially provided for by this Convention¹²⁸

This concept of national treatment means that each country that is a party to the Paris Convention must grant the same protection it grants to its own nationals to nationals of other member countries.¹²⁹

This means that there is no requirement of reciprocity.¹³⁰ This national treatment rule protects foreigners and guarantees that they will not be discriminated against in any way.¹³¹ In the world of data protection, this means the Paris Convention is at least one antidote for bias based on residence.

(f) European Database Directive

As noted above, in contrast to the United States, the EU provides a *sui generis* right in databases. This right was created by the Database Directive 96/9/EC.¹³² The Database Directive protects unoriginal databases in which there has been substantial investment and is distinguished from copyright protection, which grants protection in databases based on the author's own

125 Paris Convention, article 1(3).

126 Paris Convention, article 10(1).

127 Paris Convention, article 10 *bis*.

128 Paris Convention, article 2(1).

129 "International Treaties and Conventions on Intellectual Property", *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 242.

130 "International Treaties and Conventions on Intellectual Property", *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 243 ("Supposing that a given member country has a longer term of patent protection than another member country: the former country will not have the right to provide that nationals of the latter country will enjoy a term of protection of the same length as the term of protection is in the law of their own country").

131 Paris Convention, article 242.

132 Directive 96/9 EC of the European Parliament and of the Council on the Legal Protection of Databases, 11 March 1996, O.J. (L 77/20).

intellectual creation through original selection or arrangement of its contents, i.e.,¹³³ copyright protects the structure of the database and the *sui generis* right protects the data in the database, irrespective of the copyrightability of the data.¹³⁴

The European Court of Justice has qualified the notion of substantial investment by holding that investment in the creation of the data in the database cannot be considered. Rather, the term “substantial investment in either the obtaining, verification or presentation of the contents” refers to seeking out independent materials and collecting them, ensuring the reliability of the information, monitoring the database for its accuracy, and arranging the data.¹³⁵ It is important to note that, unlike copyright, *sui generis* is not an exclusive right; others are not prohibited from independently gathering the same data from other original sources.¹³⁶

The Database Directive defines a database “as a collection of independent works, data, or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means”.¹³⁷ The European Parliament and the Council of the European Union recognize that databases are a “vital tool in the development of an information market”¹³⁸ and that the creation of “databases requires the investment of considerable human, technical, and financial resources while such databases can be copied or accessed at a fraction of the cost needed to design them independently”.¹³⁹

Furthermore, as databases are “not sufficiently protected”¹⁴⁰ and there is an “absence of a harmonized system of unfair-competition legislation” to protect database owners from “unauthorized extraction and/or re-utilization of the contents of a database”,¹⁴¹ the Directive is a “means to secure the remuneration of the maker of the database”.¹⁴² While the Database Directive “afford[s] an appropriate and uniform level of protection [to] databases”, its

133 Stephens, “Database Rights: A Surprise Judgment by the European Court of Justice”, 18 *World Intell. Prop. Rep.* 12 (1 December 2004).

134 Grosheide, “Database Protection — The European Way”, 8 *Wash. U. J.L. & Pol’y* 39, at p. 40 (2002).

135 Stephens, “Database Rights: A Surprise Judgment by the European Court of Justice”, 18 *World Intell. Prop. Rep.* 12 (1 December 2004).

136 Stephens, “Database Rights: A Surprise Judgment by the European Court of Justice”, 18 *World Intell. Prop. Rep.* 12, at p. 45 (1 December 2004).

137 Directive 96/9 EC, article 1(2).

138 Directive 96/9 EC, Recital 9.

139 Directive 96/9 EC, article 7.

140 Directive 96/9 EC, article 1.

141 Directive 96/9 EC, article 6.

142 Directive 96/9 EC, article 48.

provisions “are without prejudice to data protection legislation”, specifically Directive 95/46/EC “on the protection of individuals with regard to the processing of personal data and on the free movement of such data”.¹⁴³

The Database Directive prohibits the “temporary or permanent reproduction by any means and in any form, in whole or in part” of the database, in addition to “translation, adaptation, arrangement and any other alteration”, and “any form of distribution to the public of the database or of copies thereof”.¹⁴⁴ However, after the first sale of a copy of the database, the right to control the resale of that copy is exhausted.¹⁴⁵

Exceptions to the *sui generis* right exist for non-commercial use as an illustration for teaching or scientific research, and for use for the purposes of public security or administrative or judicial procedure.¹⁴⁶ Additionally, the term of protection granted under *sui generis* is limited to 15 years from the date of completion or from the date of substantial change resulting from substantial new investment.¹⁴⁷

(g) Criminal Law

Criminal laws also weigh in on the side of intellectual property rights holders, but they are far less harmonized. For example, the United States Federal Communications Act protects intellectual property rights holders in radio or satellite cable programming from unauthorized interception and publication.¹⁴⁸ Willful violators of the Act are subject to a fine of up to US \$2,000 and/or six months’ imprisonment;¹⁴⁹ however, if the violation is for private or commercial financial gain, the penalties increase to up to US \$50,000 and/or two years’ imprisonment for the first violation.¹⁵⁰

Another United States law is the Federal Communications Act. It also contains a special provision for violations that involve a “device or equipment [that] is primarily of assistance in the unauthorized decryption of satellite cable programming” which, for each violation, calls for fines of up to US \$500,000 and/or up to five years in prison.¹⁵¹

143 Directive 96/9 EC, article 48.

144 Directive 96/9 EC, article 5.

145 Directive 96/9 EC, article 5(c).

146 Directive 96/9 EC, article 6.

147 Directive 96/9 EC, article 10.

148 47 United States Code, section 605(a).

149 47 United States Code, section 605(e)(1).

150 47 United States Code, section at 605(e)(2). The penalty for subsequent convictions increases to up to US \$100,000 and/or five years’ imprisonment.

151 47 United States Code, section 605(e)(4).

Lastly, the United States Anti-Counterfeiting Amendments Act of 2004 is part of a larger regime aimed at preventing the counterfeiting of copyrighted works and phonorecords.¹⁵² The penalty for affixing illicit or counterfeit labels to, among others, a copy of a computer program, motion picture, literary work, or documentation or packaging is a fine and/or imprisonment for up to five years.¹⁵³

(h) Contract Law

One cannot discuss protection of data unless one addresses self-help measures available to intellectual property rights owners. In the United States and elsewhere, contract law is often used by intellectual property rights holders to protect their digital works. The contracts take the form of licenses, with “shrink wrap” and “click on” licenses being the most common because they require the end user to accept the conditions of the license as a condition of installing and using the program.¹⁵⁴

While the “freedom to contract” is a powerful rights enforcement tool, a contract does not create exclusive rights and, as such, it only affects the parties to the contract and not others.¹⁵⁵ Furthermore, contracts run the risk of being preempted by national law or international treaty.¹⁵⁶ Such preemption may occur when the contract, for example, exceeds the limitations of copyright law by prohibiting fair use or violating the first-sale doctrine.¹⁵⁷

Another method of self-help is maintaining information in secret and not disclosing it as a means of protecting against misappropriation. If the information has value, it may be a trade secret.¹⁵⁸ So long as the information has value, is maintained as a secret, and is not generally known to the industry, trade secrets serve as the primary alternative form of intellectual property rights protection to patents.¹⁵⁹

Trade secrets legislation protects the intellectual property rights owner against misappropriation of trade secrets through improper means.¹⁶⁰ In the

152 Intellectual Property Protection and Courts Amendments Act of 2004, Pub. L. Number 108-482 2004 H.R. 3632 (2004).

153 Intellectual Property Protection and Courts Amendments Act of 2004, Pub. L. Number 108-482 2004 H.R. 3632 (2004). An illicit label is a genuine document or certificate that is used to verify the authenticity of a copy that has been altered or misused.

154 Leaffer, *Understanding Copyright Law* (3d ed., 1999), at p. 25.

155 Leaffer, *Understanding Copyright Law* (3d ed., 1999), at p. 493.

156 Leaffer, *Understanding Copyright Law* (3d ed., 1999), at p. 489.

157 Leaffer, *Understanding Copyright Law* (3d ed., 1999), at p. 493.

158 United States Uniform Trade Secrets Act, section 1(4) (amended 1985).

159 Adelman *et al.*, *Cases and Materials on Patent Law* (1998), at p. 51.

160 United States Uniform Trade Secrets Act, sections 1(2) and 3.

United States, damages for misappropriation include both actual losses and the unjust enrichment caused by the misappropriation, or the cost of a reasonable royalty, plus, in the case of willful and malicious misappropriation, exemplary damages and reasonable attorney's fees.¹⁶¹

In Civil Law jurisdictions, unfair competition protects against the misconduct of the one who appropriates the contents from a database under a form of tortious liability for the value of the data or information. In Common Law jurisdictions, misappropriation law applies to prevent one business from "passing off" its goods or services as those of another.¹⁶² In either type of jurisdiction, the intellectual property rights holder must prove the tortious act, which typically requires more than just evidence of direct copying.¹⁶³

Thus, while the intellectual property rights regimes of the world are more and more becoming a single fabric, the fabric is more like a quilt of national variations on a theme imposed through international treaties. So long as each national variation is enforced fairly and consistently, the promise of innovation's reward and the societal benefits from the free flow of innovation can co-exist and flourish.

2.05 Legal Factors in Protecting Privacy

(a) Criminal Laws

Personal data protection laws have taken on various shapes and hues. At its most fundamental is the right of a person to be protected against the theft of his identity. For example, the Identity Theft Penalty Enhancement Act in the United States establishes the crime of aggravated identity theft for the unauthorized transfer, possession, or use of another person's means of identification during the course of certain enumerated felonies, which generally relate to fraud, nationality, and citizenship.¹⁶⁴

However, identity theft is just one form of harm that can flourish unless limits are placed on what one may do with the private information concerning another. Not surprisingly, beyond the restrictions on identity theft are a host of laws that apply to protection afforded to the privacy of personal information. Those protections fall into two categories, these being restrictions on government and restrictions on private parties. Both categories are evolving.

161 United States Uniform Trade Secrets Act, sections 3 and 4.

162 rosheide, "Database Protection—The European Way", 8 *Wash. U. J.L. & Pol'y* 39, at p. 45; Leaffer, *Understanding Copyright Law* (3d ed., 1999) at p. 38.

163 Grosheide, "Database Protection—The European Way", 8 *Wash. U. J.L. & Pol'y* 39, at p. 45.

164 Identity Theft Penalty Enhancement Act of 2004, Pub. L. Number 108-275, section 2, H.R. 1731 (2004).

(b) Privacy Act of Canada

An example of restrictions on the government's handling of personal data is the Privacy Act of Canada, which regulates personal information about individuals held by a government institution and provides individuals with a right of access to that information.¹⁶⁵ Personal information under the Canada Privacy Act includes information about an identifiable individual that is recorded in any form, including race, national or ethnic origin, color, religion, age, marital status, information relating to education, medical, financial, criminal, or employment history, and any identifying numbers, symbols, or marks assigned or ascribed to the individual, such as address, fingerprints, or blood type.¹⁶⁶ The regulations place limits on the collection, use, and disclosure of this information by specifying that:

1. Any information collected must relate directly to a program or activity of the government institution,¹⁶⁷
2. The individual must be informed of the collection and the use of the information,¹⁶⁸
3. The information must be used for the purpose for which the information was obtained;¹⁶⁹ and
4. The individual must consent to any other use or disclosure, except as provided by the Act.¹⁷⁰

The Privacy Act of Canada allows Canadians to:

1. Access any relevant personal information which is under the control of the government;
2. Request that omissions or errors be corrected;
3. Have the request for correction, if not granted, noted on the information; and
4. Require that the correction, or the denied request for correction, be given to anyone to whom the personal information was disclosed within the two years prior to the request for correction.¹⁷¹

165 Privacy Act of Canada (1980–1983), c. 111, sched. II.

166 Privacy Act of Canada, section 3.

167 Privacy Act of Canada, section 5(1).

168 Privacy Act of Canada, section 5(2).

169 Privacy Act of Canada, section 7(a).

170 Privacy Act of Canada, sections 7 and 8(1).

171 Privacy Act of Canada, section 12.

The Governor in Council has the authority to extend the right of access to non-citizens and to set conditions on the right of access as the Governor in Council deems appropriate.¹⁷²

(c) United States Privacy Act

In a similar fashion, the United States Privacy Act of 1974¹⁷³ requires government agencies to publish notices in the Federal Register on the establishment or revision of systems of records, to account for disclosures of certain records, and to agree in writing with another agency before entering into a computer matching program, and to provide individuals access to records maintained about them.¹⁷⁴

Privacy-related concerns impact national security laws and programs. For example, funding legislation for the United States Department of Homeland Security requires that technology used to screen aviation passengers and identify those who may pose a security threat must, prior to deployment:

1. Contain safeguards to prevent abuse and unauthorized access;
2. Address any privacy concerns posed by its system architecture; and
3. Provide a system of due process whereby targeted passengers can appeal the determination and correct any erroneous information that facilitated the false determination.¹⁷⁵

In addition to privacy controls implemented as a condition of funding, the United States Department of Homeland Security has a statutorily required Privacy Officer.¹⁷⁶ This Privacy Officer's primary responsibility is over the United States Department of Homeland Security privacy policy, which includes assuring that the use, collection, and disclosure of personal information by the United States Department of Homeland Security complies with the Privacy Act and ultimately sustains, and does not erode, established privacy protections.¹⁷⁷

However, national security and law enforcement must, to some extent, erode privacy protections. Two exceptions to the Privacy Act of Canada illustrate

172 Privacy Act of Canada, section 12(3).

173 5 United States Code, section 552(a).

174 Homeland Security Privacy Office Report on Privacy and Protecting Our Homeland, Report to Congress, at p. 11 (April 2003–June 2004).

175 Department of Homeland Security Appropriations Act, Pub. L. Number 108-3342, section 522(a), 2004 H.R. 4567 (18 October 2004).

176 Homeland Security Privacy Office Report on Privacy and Protecting Our Homeland, Report to Congress, at p. 1 (April 2003–June 2004).

177 Homeland Security Act of 2002, Pub. L. Number 107-296, section 222, 116 Stat. 2155 (2002).

this point. First, government institutions are not obligated to inform the individual of the purpose of the information collection if the notice of such collection may jeopardize the accuracy of the information collected or defeat the purpose or prejudice the use for which the information is collected.¹⁷⁸ Second, government institutions may deny the right of access to personal information contained in an “exempt bank”.¹⁷⁹ Exempt banks are designated as such by the Governor in Council and are repositories of personal information that, in general, relates to national security or law enforcement.¹⁸⁰

(d) European Data Protection Directive

Shifting to restrictions on private entities, one must begin with the seminal archetype of privacy legislation, Directive 95/46/EC, the EU Data Protection Directive. The Data Protection Directive guarantees the protection of individuals with regard to the processing of personal data and its free movement across borders. It states as its objective “protect[ing] the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”; however, the enforcement of such rights “shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded” to natural persons.¹⁸¹

The Data Protection Directive establishes the conditions under which the processing of personal data is lawful.¹⁸² Under the Directive, “personal data” means any information relating to an identified or identifiable natural person and which data can directly or indirectly identify the person, whether by an identification number or physical attributes. The “processing of personal data” includes any:

... operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ...¹⁸³

Additionally, the Directive applies to both electronic information and manual records that are part of a structured filing system.¹⁸⁴

178 Privacy Act of Canada, section 5(3).

179 Privacy Act Canada, section 18(2).

180 Privacy Act of Canada, sections 21 and 22.

181 Directive 95/46/EC, article 1.

182 Directive 95/46/EC, article 5.

183 Directive 95/46/EC, article 2(6).

184 Privacy Office at www.dataprivacy.i.e./4aii.htm (2005) (Ireland).

Under the Directive, “personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”.¹⁸⁵ Prior to processing personal data, the data subject must “unambiguously give . . . his consent”,¹⁸⁶ unless certain narrow exceptions are met, such as the “processing is necessary for the performance of a contract to which the data subject is party”.¹⁸⁷ Processing of data in special categories, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life is strictly prohibited, unless the data subject has given his explicit consent or the processing is absolutely necessary.¹⁸⁸

One notable point of distinction of the Data Protection Directive is that individuals have the right to deny consent to be:

. . . subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, and conduct.¹⁸⁹

Data subjects also can object to the processing of their data for direct marketing activities.¹⁹⁰

The Directive lays out additional fundamental principles. The data subject must be provided with the information necessary to guarantee the fair processing of the data collected, including the identity and contact information of the entity controlling the information (“data controller”) and the purposes of the processing for which the data are intended.¹⁹¹ Furthermore, the data controller must provide the data subject access to the data in order, generally, to confirm that the data is accurate and is being processed as disclosed and in conformance with the Directive.¹⁹²

Personal data must be kept confidential and secure during processing as to prevent “accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access . . . and all other unlawful forms of processing”.¹⁹³ The data controller is obligated to make its processing operations transparent and to make them public by registering the operations with the proper national authority.¹⁹⁴

185 Directive 95/46/EC, article 61(b).

186 Directive 95/46/EC, article 7(a).

187 Directive 95/46/EC, article 7(b).

188 Directive 95/46/EC, article 8.

189 Directive 95/46/EC, article 15.

190 Directive 95/46/EC, article 14(b).

191 Directive 95/46/EC, articles 10, 11, and 19.

192 Directive 95/46/EC, article 15.

193 Directive 95/46/EC, articles 16 and 17.

194 Directive 95/46/EC, article 21.

The national authority is then responsible for determining if any risks to the rights and freedoms of the data subjects are present.¹⁹⁵ Finally, the Directive mandates that the member states provide remedies to data subjects for any breach of the rights guaranteed to the data subjects by the applicable national law, including the entitlement to receive compensation for actual damages and sanctions for infringement of the provisions of the Directive.¹⁹⁶

Article 25 of the Directive prohibits the transfer of personal data to a third country unless the third country ensures an adequate level of protection, as compared to the Directive and as determined by the Commission. The Commission has published standard contractual clauses to facilitate data flows from the Community where the third country has unequal data protection standards.¹⁹⁷ As expected, the contract clauses mirror the Principles of the Directive; however, they specifically exclude punitive damages¹⁹⁸ and give an opportunity to cure allegations of breach of duty.¹⁹⁹

The clauses also give the data subject the right “to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses”,²⁰⁰ which would seem to imply that the data exporter has an obligation to audit the data importer’s practices.

(e) Personal Information Protection and Electronic Documents Act of Canada

The Directive served as the model for Canada’s legislative protections with respect to regulation of private entities and, as such, the Canadian legislation contains the same basic privacy principles:²⁰¹

For the purposes of article 25(2) of Directive 95/46/EC, Canada is considered as providing an adequate level of protection for personal data

195 Directive 95/46/EC, article 20.

196 Directive 95/46/EC, articles 22, 23, and 24.

197 Commission Decision Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Contractual Clauses for the Transfer of Personal Data to Third Countries, 27 December 2004.

198 Commission Decision Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Contractual Clauses for the Transfer of Personal Data to Third Countries, clause III(a).

199 Commission Decision Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Contractual Clauses for the Transfer of Personal Data to Third Countries, clause III(b).

200 Commission Decision Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Contractual Clauses for the Transfer of Personal Data to Third Countries, clauses II(g) and III(b).

201 Singh, “Lack of Minimum Global Privacy Standard Said to Impair Outsourcing, Online Business”, 10 *Elec. Commerce & L.* 7 (16 February 2005).

transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documents Act.²⁰²

The Personal Information Protection and Electronic Documents Act of Canada applies to all personal information collected, used, or disclosed by private sector organizations in the course of commercial activity.²⁰³

The Act sets out a series of obligations, found in Schedule I to the Act, which are based on the 10 Privacy Principles of the Code, as set out in the national standard of Canada, the Model Code for the Protection of Personal Information.²⁰⁴ The Privacy Principles are:

. . . accountability, identifying the purposes for the collection of personal information, obtaining consent, limiting collection, limiting use, disclosure and retention, ensuring accuracy, providing adequate security, making information management policies readily available, providing individuals with access to information about themselves, and giving individuals a right to challenge an organization's compliance with these principles.

The Personal Information Protection and Electronic Documents Act of Canada holds private organizations accountable for the personal information under their control.²⁰⁵ The accountability extends to information that has been transferred to a third party, even if that party is located outside the borders of Canada. Additionally, the accountability applies to information that will not be “used”, but merely “processed” under a business outsourcing agreement.²⁰⁶

As a result, organizations transferring personal information are required to “use contractual or other means to provide a comparable level of protection while the information is being processed by a third party”.²⁰⁷ This means that the private organization in Canada must ensure, prior to any transborder transfer, that the

202 Commission Decision Pursuant to Directive 95/46 EC of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act, 20 December 2001.

203 Personal Information Protection and Electronic Documents Act, section 4. The Personal Information Protection and Electronic Documents Act also applies to employment records collected, used, or disclosed in connection with a federally regulated industry, such as banking and railroad, ship, or air transportation.

204 Personal Information Protection and Electronic Documents Act, Summary and Schedule 1.

205 Personal Information Protection and Electronic Documents Act of Canada, Schedule 1, section 4.1.

206 Personal Information Protection and Electronic Documents Act of Canada, Schedule 1, section 4.1.3.

207 Personal Information Protection and Electronic Documents Act of Canada, Schedule 1, section 4.1.3.

third party in another country will provide a level of protection comparable to that which the personal information would receive in Canada.²⁰⁸

Of course, the general rule in Canada is that any collection, use, or disclosure of personal information by a private commercial entity can only occur if all the requirements of the Personal Information Protection and Electronic Documents Act have been met.²⁰⁹ A primary concern with cross-border transfers of personal information is security and the prevention of unauthorized access or disclosure.²¹⁰

For example, a problem is presented when the transferee is located in a country where the laws permit certain disclosures to that country's government or law enforcement agencies in a manner not authorized by the Personal Information Protection and Electronic Documents Act. The foreign third party transferee will not be able to contract against the local law; therefore, because the transferor in Canada has a duty to protect personal information under its control from unauthorized disclosure, it may find that the transfer is not permissible.²¹¹

(f) Other Regimes

However, not all privacy regimes follow the same path. Indeed, for example, a wholly different regime exists in Argentina. Argentina requires Argentine and foreign companies doing business in Argentina to register all databases, whether in electronic or hard-copy format, that contain personal data that is shared with third parties and is subject to treatment or processing.²¹² This registry was implemented as part of the Habeas Data Law and applies to for-profit and not-for-profit transfers of personal data.

Under the law, all individuals and legal entities must provide detailed information on, for example, the kind of data their databases contain, what their purpose is, the means and place of storage, how the information was obtained, as well as safekeeping measures.²¹³

208 Report on Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, section 4 (October 2004).

209 Personal Information Protection and Electronic Documents Act, section 4(1)(a).

210 Personal Information Protection and Electronic Documents Act, section 4.7.1.

211 Other laws, treaties, or agreements or memorandums of understanding between the originating country and the specific governments and law enforcement agencies may exist that would otherwise authorize the transfer. Generally, these overriding exceptions are specific to the industry involved, such as commercial airlines.

212 Haskel, "Argentina Implements Mandatory Registration Requirement for Databases", 4 *Privacy & Sec. L.* 9 (28 February 2005).

213 Haskel, "Argentina Implements Mandatory Registration Requirement for Databases", 4 *Privacy & Sec. L.* 9 (28 February 2005).

The legislation bans transferring database contents to third parties without written consent from the individuals involved. The request must indicate the reasons why the handover is necessary. This applies even if the transfer is between different locations of the same company. However, when transfer of the data is necessary to render adequate services, a contact pledging to honor the data privacy may suffice.²¹⁴

Habeas Data is a constitutional right granted in several countries in Latin America, which translated means “you should have the data”. In general, the right “is designed to protect, by means of an individual complaint presented to a constitutional court, the image, privacy, honor, information self-determination and freedom of information of a person”.²¹⁵

Despite its differences as compared to the EU regime:

... [f]or the purposes of article 25(2) of Directive 95/46/EC, Argentina is regarded as providing an adequate level of protection for personal data transferred from the Community.²¹⁶

(g) National Inconsistencies

Despite the fact that many nations offer an “adequate level of protection for personal data”, yet, inconsistencies abound. For example, the Privacy Act of Canada, which regulates the collection, use, and disclosure by governmental institutions of personal information, does not require the same safeguards to prevent the unauthorized disclosure of personal information about Canadians as a result of a cross-border transfer.²¹⁷

The potential impact of the transborder flow of information was raised when the British Columbia Government and Services Employees’ Union challenged the British Columbia Ministry of Health Services when it sought to outsource the administration of British Columbia’s public health insurance program to a US-linked private service provider.²¹⁸

214 Haskel, “Argentina Implements Mandatory Registration Requirement for Databases”, 4 *Privacy & Sec. L.* 9 (28 February 2005).

215 Guadamuz, “Habeas Data: The Latin-American Response to Data Protection”, 2000 *J. Info, L. & Tech.*, at <http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html>.

216 Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina, article 1, 30 June 2003.

217 Report on Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, at p. 10 (October 2004) (other legislation or contractual agreements may provide limited protection).

218 Report on Privacy and the USA Patriot Act; Implications for the British Columbia Public Sector Outsourcing, Information and Privacy Commissioner for British Columbia, at p. 23 (October 2004). The challenge has been presented to the British Columbia Supreme Court and was scheduled to be heard in March 2005. The petition and associated affidavits can be found at <http://www.bcgeu.ca/index.php4?id=2093>.

The provincial government is also seeking to privatize its revenue and tax services, and the union is concerned that a wide range of detailed financial records will be exposed to potential scrutiny by the United States Federal Bureau of Investigation (FBI) and other United States government agencies.²¹⁹

This case points up “a nearly universal misconception that the United States has no privacy framework that might be viewed as consonant with those of other countries”.²²⁰ Additionally, there is a:

... perception that the US interest in privacy protection and privacy rights may be parochial, isolated to Americans only, fueling the misperception of United States non-comparability with basic information privacy protections afforded in many other regions of the world to any individual, regardless of status.²²¹

In an effort to address this concern, the United States Department of Homeland Security has entered into more stringent privacy agreements with other entities and incorporated enhanced privacy procedures. For example, a recent posting in the Federal Register stated that “[w]hile non-United States persons are not covered by the Privacy Act, such persons will still be afforded the same access and redress remedies” as United States persons by contesting and seeking amendment of records kept through the United States Department of Homeland Security Privacy Office.²²²

While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences, many United States organizations have expressed uncertainty about the impact of the EU-required “adequacy standard” on personal data transfers from the European Union to the United States.²²³ For now, these differences are resolved through a safe

219 “British Columbia Government and Service Employee’s Union, Latest Government Records Privatization Deal a Further ‘Betrayal’ Charges BCGEU”, paragraph 2 (26 November 2004), at www.bcgeu.ca/2583. British Columbia Government and Service Employee’s Union, Quick Facts, Powers of the USA Patriot Act (6 August 2004) at www.bcgeu.ca/index4?id=2440.

220 Homeland Security Privacy Office Report on Privacy and Protecting our Homeland, Report to Congress, at p. 11 (April 2003–June 2004).

221 Homeland Security Privacy Office Report on Privacy and Protecting our Homeland, Report to Congress, at p. 11 (April 2003–June 2004).

222 68 Fed. Reg. 148, at p. 45269 (1 August 2003) (regarding contesting records for Computer Assisted Passenger Prescreening System, CAPPS II).

223 Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the United States Department of Commerce at Annex 1 (26 July 2000).

harbor program where United States companies can voluntarily agree to abide by the principles by certifying adherence to the United States Department of Commerce and publishing their privacy policies.

For the purposes of article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the “Safe Harbor Privacy Principles” (hereinafter “the Principles”), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the Frequently Asked Questions issued by the United States Department of Commerce on 21 July 2000, as set out in Annex II to this Decision, are considered to ensure an adequate level of protection for personal data transferred from the Community to organizations established in the United States.²²⁴

In short, the safe harbor requires that a United States company provide conspicuous notice to individuals about the purposes for which it collects and uses personal data. Included in that notice should be information on how to contact the company with inquiries and complaints, the types of third parties to which it discloses the information, and choices available to the individual for limited disclosure.²²⁵

Additionally, the company must offer individuals an opportunity to opt out from third-party disclosure and from having the information used for a purpose that is incompatible with the original purpose of collecting the data. The company can then transfer the information to a third party only if that party either subscribes to the Principles itself or if the company enters into a written agreement with the third party where the third party is bound to provide at least the same level of privacy protection as is required by the Principles.²²⁶

The company also must take reasonable precautions to protect the data’s security and integrity, i.e., that the data is reliable for its intended use, accurate, complete, and current. Finally, the company must provide individuals

224 Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the United States Department of Commerce at Annex 1 (26 July 2000).

225 Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the United States Department of Commerce at Annex 1 (26 July 2000).

226 Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the United States Department of Commerce at Annex 1 (26 July 2000).

access to their information and must provide recourse to individuals' complaints regarding the company's adherence to the Principles.²²⁷

The United States is likely to undergo a waive of legislation regarding the collection, sale, and disclosure of personally identifiable information due to the recent incident where the data broker ChoicePoint, Inc., sold information to criminals posing as legitimate business customers of ChoicePoint.²²⁸

ChoicePoint gathers information on millions of people and is the largest data broker in the United States. As a result of this incident, ChoicePoint sent notice to 145,000 individuals in the United States telling them that their personal information had been improperly accessed.²²⁹ Within the United States, the State of California is the only state that requires such notice.²³⁰

(h) Exceptions

Exceptions to privacy laws abound. The Privacy Act of Canada allows government institutions to disclose personal information for a purpose other than the original use for which the information was obtained, without the consent of the individual to whom it relates, when other laws or regulations permit the disclosure,²³¹ in response to a court order²³² or, in general, for the purpose of enforcing any law of Canada²³³ or when the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.²³⁴

The Personal Information Protection and Electronic Documents Act of Canada provides that organizations may disclose personally identifiable information without the knowledge or consent of the individual only if the disclosure qualifies as one of the specifically enumerated statutory exceptions.²³⁵ These exceptions allow disclosure, for example, to comply with a

227 Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the United States Department of Commerce at Annex 1 (26 July 2000).

228 Tumey, *et. al.*, "State, Federal Response Triggered By ChoicePoint Data Breach Incident", 10 *Elec. Commerce & L.* 9 (2 March 2005).

229 Mahoney, "Data Broker Warns 145,000 Consumers Of Security Breach, Potential Identity Theft", 10 *Elec. Commerce & L.* 8 (23 February 2005).

230 "Leahy Calls for Senate Judiciary Probe On Government, Industry Data Collection", 10 *Elec. Commerce & L.* 9 (2 March 2005).

231 Privacy Act of Canada, section 8(2)(b).

232 Privacy Act of Canada, section 8(2)(c).

233 Privacy Act of Canada, section 8(e).

234 Privacy Act of Canada, section 8(m)(i).

235 Personal Information Protection and Electronic Documents Act of Canada, section 7(5).

court order,²³⁶ for research when obtaining consent is impracticable and the purposes of the research cannot be achieved without disclosure,²³⁷ in cases of emergency that threaten the life, health, or security of an individual,²³⁸ and when a government authority requests disclosure of the information as part of enforcing any law of Canada²³⁹ or ensuring national security.²⁴⁰

Article 13 of the EU Data Protection Directive provides exemptions, for example, for national security, defense, public security, criminal investigations, and important economic or financial interest of a member state or of the European Union, including monetary, budgetary, and taxation matters.²⁴¹

2.06 New Tools, New Enforcement Questions

(a) In General

Intellectual property rights and privacy rights are only as viable as they are enforceable. Data protection is relatively new and least consistently applied globally, while intellectual property rights have a rich history of enforcement buttressed by a wealth of international treaties.

Generally, the first step in enforcing data protection laws is for the data subject to file a complaint with his national Privacy or Data Protection Commissioner.²⁴² This is a primary purpose for the public registries.²⁴³ Although premised on a private right to complain, personal data protection laws are increasingly enforced by government agencies.

(b) Other Statutory Monitoring, Privacy Impact Assessments

(i) *United States Privacy Impact Assessment*

In other instances, the government agency is proactive. The United States E-Government Act of 2002, section 208, mandates a Privacy Impact Assessment

236 Personal Information Protection and Electronic Documents Act of Canada, section 7(3)(c).

237 Personal Information Protection and Electronic Documents Act of Canada, section 7(3)(f).

238 Personal Information Protection and Electronic Documents Act of Canada, section 7(3)(e).

239 Personal Information Protection and Electronic Documents Act of Canada, section 7(3)(c.1)(i) and 7(3)(d)(ii).

240 Personal Information Protection and Electronic Documents Act of Canada, section 7(3)(c.1)(ii) and 7(3)(d)(i).

241 Directive 95/46 EC, article 13.

242 Privacy Office, at www.dataprivacy.i.e./2.htm (Data Protection: Your Rights 2005) (Ireland).

243 Privacy Office, at www.dataprivacy.i.e./2.htm (Data Protection: Your Rights 2005) (Ireland).

(PIA) for all federal agencies when there are new collections of, or new technologies applied to, personally identifiable information. The purpose of a PIA is to ensure that information technology systems of the federal government are maintained in conformity with fair information principles concerning notice, consent, access, redress, data integrity, and security.²⁴⁴

For example, the United States Department of Homeland Security Privacy Office is statutorily required to evaluate all new technologies used in the furtherance of its security mission for their impact on personal privacy and to provide an annual report to Congress on the Department's activities that affect privacy.²⁴⁵ This report includes complaints of privacy violations and an evaluation of the Department's internal controls.²⁴⁶ Additionally, the United States Department of Homeland Security Privacy Office investigates data sharing and data mining practices and reports its conclusions to Congress.²⁴⁷

Separately, the Homeland Security Act provides that the United States Department of Homeland Security Privacy Officer conduct PIAs that address the type of personal information collected and the number of people affected for proposed rules of the Department of Homeland Security²⁴⁸ because:

... [e]ven when actual Privacy Act violations are not found, it is nevertheless important that clear rules be in place to ensure that information sharing is done in a legitimate, respectful, and limited way.²⁴⁹

(ii) *Canada Privacy Commissioner Audit*

The Personal Information Protection and Electronic Documents Act of Canada gives the Privacy Commissioner the authority to audit the personal information management practices of a private organization if it reasonably believes that the organization is not following the Act.²⁵⁰ Following the audit, the Commissioner must report the findings to the organization and

244 United States E-Government Act of 2002, section 24.

245 Homeland Security Act of 2002, Pub. L. Number 107-296, section 222(1), H.R. 5005 (2002). Homeland Security Privacy Office Report on Privacy and Protecting Our Homeland, Report to Congress, at p. 1 (April 2003–June 2004).

246 Homeland Security Act of 2002, Pub. L. Number 107-296, section 222(5), H.R. 5005 (2002).

247 Homeland Security Privacy Office Report on Privacy and Protecting Our Homeland, Report to Congress, at p. 11 (April 2003–June 2004).

248 Homeland Security Act of 2002, Pub. L. Number 107-296, section 222(4), H.R. 5005 (2002).

249 Homeland Security Privacy Office Report on Privacy and Protecting Our Homeland, Report to Congress, at p. 10 (April 2003–June 2004).

250 Personal Information Protection and Electronic Documents Act, section 18(1).

may make recommendations.²⁵¹ While it is unlawful to knowingly obstruct the audit,²⁵² the enforcement authority of the Commissioner is limited.²⁵³

The Commissioner may then make public any information relating to the personal information management practices of the organization if the Commissioner deems it in the public interest to do so.²⁵⁴ The Commissioner may also include this information in the annual report to Parliament.²⁵⁵

(c) Digital Rights Management

(i) In General

In contrast to an aggrieved data subject, intellectual property rights owners have had a traditional array of enforcement tools available through the civil justice systems of the intellectual property rights regimes under which they enjoy rights. Yet, that array is increasingly viewed as too slow, cumbersome, and expensive to be effective. Intellectual property rights holders, therefore, are increasingly turning to digital rights management as the primary method of battling online infringement.²⁵⁶

Electronic copyright management systems, or digital rights management, generally identify technologies, or technical protection measures, that allow an intellectual property rights holder to control and restrict the use of his or her work when it is in an electronic form. Digital rights management opponents chidingly call this term “digital restrictions management” because they claim the protection measures often exceed the owner’s rights in the underlying work.²⁵⁷

Digital rights management includes not only software, but hardware as well. Through “Trusted Computing” or “Secure Engineering”, intellectual property rights holders are developing microprocessor-based devices that use

251 Personal Information Protection and Electronic Documents Act, section 19(1).

252 Personal Information Protection and Electronic Documents Act, section 28.

253 The court has authority to order, in addition to other remedies, an organization to correct its practices; however, under the Act, it appears that investigations initiated by the Commissioner are not eligible for court hearings. Personal Information Protection and Electronic Documents Act, articles 11 and 14.

254 Personal Information Protection and Electronic Documents Act, section 20(2).

255 Personal Information Protection and Electronic Documents Act, section 25.

256 “EC Privacy Advisors Warn That IP Enforcers Could Be Skirting Data Protection Directive”, 10 *Elec. Commerce & L.* 6 (9 February 2005).

257 For example, the *bona fide* purchaser of a *bona fide* copy of the work may be prevented from selling the copy purchased, as would otherwise be allowed under the “first sale doctrine” which, in the United States, is codified at 17 United States Code, section 109. The statute states, in part that “the owner of a particular copy . . . lawfully made . . . is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy . . .”. Additionally, there have been claims that digital rights managements have been used to place restrictions on works in the public domain.

both hardware and software to protect digital intellectual property.²⁵⁸ Other methods of digital rights management include technologies for identification, metadata, rights expression language, encryption, persistent association, privacy, and payment, all of which create a secure environment for the delivery of intellectual property rights-based content.²⁵⁹ These technologies closely track the digital content and the user to ensure that the content is used according to the intellectual property rights holder's pre-determined conditions.

(ii) *United States, the Digital Millennium Copyright Act*

In the United States, the Digital Millennium Copyright Act supports the use of digital rights management and provides that “no person shall circumvent a technological measure that effectively controls access to a work protected” under the copyright law.²⁶⁰

Two exceptions are for reverse engineering, “for the sole purpose of achieving interoperability of an independently created computer program”, and to prevent the collection of personally identifiable information that is collected “without providing conspicuous notice of such collection” and “without providing such person with the capability to prevent or restrict” the collection.²⁶¹

(iii) *European Union Copyright Directive*

The EU Copyright Directive 2001/29/EC provides similar support for digital rights management by mandating that Member States “shall provide adequate legal protection against the circumvention of any effective technological measures”.²⁶² “The Copyright Directive is broader than the Digital Millennium Copyright Act because it also prohibits acts of circumventing copyright control measures and other acts not authorized by the rights holder”, not just those used to control access to the work.²⁶³

Additionally, the Copyright Directive differs in that it provides greater leeway to private contractual agreements as opposed to enumerating specific exceptions or defenses to infringement.²⁶⁴

258 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 13.

259 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 14.

260 17 United States Code, section 1201(a).

261 17 United States Code, section 1201(f) and (i).

262 Directive 2001/29 EC, article 6.

263 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 74.

264 “International Treaties and Conventions on Intellectual Property”, *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 75.

(iv) European Union Data Protection Directive

Article 29 of the EU Data Protection Directive establishes the authority for a “Working Party” to examine the application of the Directive and to advise the Commission on any matters regarding divergences likely to affect the equivalence of protection for data subjects and the protection of persons with regard to the processing of personal data in the Community.²⁶⁵ The Working Party has issued a document with regard to data protection and intellectual property rights.²⁶⁶

It “notes that the increasing exchange of information linked to the development of the Internet touches more and more the delicate question of control over copyright protected information”.²⁶⁷ The Working Party expresses concerns over the copyright holder’s use of digital rights managements to protect his intellectual property rights “insofar as digital rights managements provide for the identification and tracing of individuals accessing legally protected information (e.g., songs, software) on the Internet” and “the possibilities available to copyright holders to enforce their rights against individuals suspected of copyright violation”.²⁶⁸

With respect to the copyright management systems, digital rights managements potentially:

... monitor ... every single act of reading, listening and viewing on the Internet by individual users thereby collecting highly sensitive information about the data subject concerned.²⁶⁹

With respect to enforcement, the Working Party notes a potential conflict between digital rights managements and legislation supporting digital rights managements, which allow intellectual property rights holders to conduct their own investigations, and privacy laws, in addition to other laws that protect fundamental rights:²⁷⁰

The Working Party calls for a development of technical tools offering privacy compliant properties, and more generally for a transparent and limited use of unique identifiers, with a choice option for the user.²⁷¹

265 Directive 95/46/EC, articles 29 and 30.

266 Article 29 Data Protection Working Party Report (18 January 2005).

267 Article 29 Data Protection Working Party Report (18 January 2005), at p. 2.

268 Article 29 Data Protection Working Party Report (18 January 2005), at p. 2.

269 Article 29 Data Protection Working Party Report (18 January 2005), at p. 3 (citing the International Working Group on Data Protection in Telecommunications, “Common Position on Privacy and Copyright Management”).

270 Article 29 Data Protection Working Party Report (18 January 2005), at p. 4.

271 Article 29 Data Protection Working Party Report (18 January 2005), at p. 8.

2.07 Impact

The tensions are very real — protection of intellectual property rights versus the public domain and the protection of privacy versus the free use of personal data (the regions above and below the diagonal in Figure 1) — requiring utmost attention to balance if transborder flow of data is to remain unobstructed. Where there is a lack of harmonization of the laws pertaining to proprietary and privacy rights, there is likely restricted transborder dataflows.

Previously, it was thought that the restrictions on these dataflows would widen the “digital divide”. However, “information and communication technologies are now in daily household use in OECD countries”, and the digital divide appears to be narrowing. Now, the OECD is concerned with the socio-economic differences that determine how people interact with information and communication technologies.

These differences are increasingly linked to unequal use, which seems to be shifting the digital divide from an “access” divide to a more complex “use divide”. The Internet amplifies social differences as new uses emerge. This suggests that attention should increasingly be paid to “how-to-use” issues.²⁷²

However, perhaps a more appropriate concern should be the “ability to use” the data. Self-help digital rights management technologies and hardware will have a profound economic impact, restricting the ability to use information products worldwide. Without harmonization of intellectual property rights and privacy regimes, intellectual property rights holders will continue to turn to protection of their digital works through digital rights management to offset failures seen elsewhere in intellectual property rights systems. This self-help measure is legally sanctioned, but some claim there are insufficient governmental regulations to temper the effects of digital rights management, as there are with intellectual property rights regimes.

Digital rights managements promote the use of non-standard equipment that is specialized to protect the data. The non-standard equipment carries with it an additional cost to potential users. Furthermore, the non-standard equipment restricts the transfer of subsequent works, if any. Thus, through a digital rights management regime, the intellectual property rights holder can obtain rights greater than that offered by traditional intellectual property rights regimes. This is because the intellectual property rights holder is establishing its own *quid pro quo*. For a price, the intellectual property rights holder will grant certain enumerated rights. The exchange, therefore, is

²⁷² “Information and Communications Technologies, OECD Information Technology Outlook 2004: Highlights”, 2004 *Sci. & Info. Tech.* 15 (December 2004), at p. 10.

limited to the intellectual property rights holder and the user and there is no contemplation of the public domain.

Digital rights management systems also expose the user to potential privacy risks. An extreme digital rights management measure may enforce control over the work through trusted computing that allows the purchaser's computer to be remotely manipulated without warning to the purchaser.²⁷³

Therefore, a side-effect of digital rights management technology is that it can collect personal data in connection with a user's purchase of a digital file in violation of international data protection directives.²⁷⁴

The legitimate purpose followed by right holders to prevent misuse of protected information often results in the tracing of users and the monitoring of their preferences. In particular, the use of unique identifiers linked with the personal information collected leads to the processing of detailed personal data.²⁷⁵

While digital rights management may create new content industries and improve on the traditional models of access to intellectual property,²⁷⁶ the varied standards and delivery mechanisms may actually hinder access. There is apprehension "that the emerging digital rights management regime is stacked against users" and that the lack of interoperability is intentional.²⁷⁷ This is not to say that all digital rights management is bad. To the contrary, it is a legally sanctioned method of preserving intellectual property rights in the whirl of our Information Age. However, like anything else, if left without proper guidance, it can be abused.

2.08 Conclusion

Harmonization of privacy and intellectual property rights laws that balance the elements shown in Figure 1 is the key to freer transborder flows of data, which in turn fuels innovation and human endeavor. Many believe "[t]he global adoption of a robust, Canadian-style privacy standard is needed to foster consumer confidence in the online medium" and "minimum

273 "International Treaties and Conventions on Intellectual Property", *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, at p. 13.

274 "EC Privacy Advisors Warn That IP Enforcers Could Be Skirting Data Protection Directive", 10 *Elec. Commerce & L.* 6.

275 Article 29 Data Protection Working Party Report, at p. 4 (18 January 2005).

276 "International Treaties and Conventions on Intellectual Property", *World Intellectual Property Organization Intellectual Property Handbook: Policy, Law, and Use*, p. 11.

277 "EC Privacy Advisors Warn That IP Enforcers Could Be Skirting Data Protection Directive", 10 *Elec. Commerce & L.* 6.

but meaningful” standards are now necessary to support cross-border outsourcing of information-based work.²⁷⁸

Any void left by privacy legislation and intellectual property laws will be filled by sanctioned self-help, which may result in data collectors and intellectual property rights owners locking up content using private tools under anti-circumvention provisions, such as those of the Digital Millennium Copyright Act, to preserve and even expand their rights without sufficient *quid pro quo*.

In summary, proprietary rights and privacy rights do not operate in a vacuum. For instance, as discussed earlier, government and private industry alike are increasing the outsourcing of their data processing. Further, an increasing percentage of “data processing” involves both personal data and other business data that ultimately in combines to forms some type of information product. These information products, as discussed earlier, give the data tremendous commercial value. This commercial value dictates that both personal data and proprietary data are in need of protection from misappropriation.

Using outsourcing as the concluding example, for harmonization to exist, the country where the outsourcing is to take place must first recognize the proprietary rights in the commercial data. Otherwise, the outsourcing company would not voluntarily risk misappropriation of the valuable data. The type of proprietary right, or specific form of intellectual property right granted, so long as it is comparable to any of the modern regimes, is not as important as the ability to enforce the right.

Second, the country where the outsourcing is to take place must then recognize the Privacy Principles in its own supporting legislation as to provide an adequate level of privacy protection. Alternatively, the entity conducting the outsourced activity may seek to be bound by contractual clauses that effectively provide an adequate level of protection. Presumably, however, the contract must be enforceable in the country where the entity conducting the outsourcing is located. Without both protection of proprietary rights in the data and protection of the privacy rights in the data, there will be a barrier preventing the transborder flow of the data to the country where the outsourcing would take place.

278 “EC Privacy Advisors Warn That IP Enforcers Could Be Skirting Data Protection Directive”, 10 *Elec. Commerce & L.* 7.

