Protection of Databases and Commercial Information in Information Societies

Anne Flanagan, BA, JD, LLM
CCLS, Queen Mary, University of London
Senior International Expert

TABLE OF CONTENTS

Executive Summary

This report considers the EU Database Directive and several other forms of protection for 'commercial information' as presented in the July 2008 EU China Information Society, Database Project Meeting and Workshop in Shanghai. It as well offers some comments on the proposed commercial data protection framework presented there by the Chinese experts.

The Database Directive

The Directive protects databases and their contents. The latter are not limited to 'commercial data' which we will consider as 'any commercially valuable data'. But as this could be stored in a database format, to the extent that the Directive protects these contents, it would be a form of protection for commercial data. The Directive protects by copyright the intellectual work of the author's creation in selecting or arranging its contents. This is not dissimilar from that protection accorded under Chinese copyright law. The sui generis right, or the database right, essentially protects the contents of databases from substantial extraction and reutilization where there was a significant investment in obtaining and verifying these contents. The sui generis right was considered a valuable protection needed to promote the development of new information products and services that the EU viewed as important to the full emergence of its Information Society. Nearly a decade later, the resulting benefits seem not to have materialized in the form of new EU origin electronic databases as per the Commission's own evaluation. It remains unclear why this is although some have suggested that this is a complex, over-protective regime and unnecessary. The lack of harmonized implementation and the restrictive analysis of some key concepts by the European Court of Justice may be other reasons. Its provisions, weaknesses and strengths are discussed further in the body of the report.

Other Means of Protecting Commercial Data

Some of the key concerns voiced about the database right were that it could lock up, for considerable times, information that might have been in the public domain or sole source

information sometimes created by public funding. It has been queried whether this posed a risk of harm to innovation and science that was justified in light of the fact that there are other ways to protect valuable information such as contract, trade secret, unfair competition laws or misappropriation, computer crime statutes and as well technology. Each of these has limitations, such as: contract law does not protect against the actions of parties not involved in a contract and trade secret requires that the information be 'secret', making it not relevant to content of databases made available to the public in whole or part by subscription, etc. Misappropriation/unfair competition is considered by some theorists as adequate to protect commercial information since it would protect only against those who would use the information competitively and allow other uses that do not. Each of these theories is also considered in turn, recognizing that while each has limitations they can also be stacked or layered together with technology to provide considerable although not perfect protection, if that exists. China's contract and unfair competition laws appear to be viable in this regard, although as with most of the other theories, requires enforcement by the parties.

Technology, notably encryption, can be a very effective way to protect information from being used if it is taken or lost. The use of technology requires some training which is viewed as an obstacle to its successful use.

It appears that in light of the perceived lacunae that these theories and technical protection present, a proposal has been made to apply certain obligations with respect to the collection, use and transmission of commercial data as a way to protect it. Although other countries protect data relating to legal entities under their personal data protection in view of perceived similar interests, e.g., ensuring that any significant decisions (an application for a service or credit) affective the legal person based on it are made with accurate, current, relevant information. This proposal seems to anticipate a full regulatory infrastructure with its ensuing costs and burdens, as any commensurate scheme. The nature and scope of these should be carefully considered as should the consequences of over protecting commercial/scientific information in a still emergent information economy. Whether this protection amounts to a legal 'propertization' of information by

virtue of it being held by commercial undertakings should be carefully considered. This is especially true of information originally available in the public domain. Thus, the definition of commercial data and the scope of the protection need be carefully defined. This also includes consideration of whether the obligations with respect to commercial data should encompass personal data held as commercially valuable data in light of their value in e commerce and the indirect costs to the economy that have been shown to arise from their inadequate security protection. The obligation for data security is very commendable. It appears limited to backing up information. Having another copy of your own data can minimize the consequences of data corruption or limited access in light of denial of service attacks where it is back up off-site. This while very valuable does not prevent breaches or data theft. Once stolen, the data can be disclosed or used by third parties. The nature of the security obligation might need to be defined in line with the intended purpose of the regulation.

Considered evaluation of these issues is suggested.

I. Introduction

This analysis is a follow-on report that encompasses and supplements the materials presented by the author on July 9, 2008[1] at the EU China Information Society meeting in Shanghai in keeping with the mission scope to explore further how commercial data is protected in the European Union. The author however, would first like to thank her most gracious hosts for their hospitality and their kind reception of her presentations. She looks forward to future meetings.

The primary focus of this part of the report is to examine the unique 'intellectual property' protection legislation, the Database Directive,[2] that the EU has crafted for certain databases that it considered were inadequately protected under then existing copyright and other laws of the Member States. In doing so it will explore why the EU considered the promulgation of this harmonizing legislation that now is part of its intellectual property *acquis communautaire* to be important and how it fit into its long-term planning for the creation of an 'information society'. This report will then provide an overview of the provisions of the Directive and will discuss some of issues that have arisen in its implementation. It will consider other ways in which commercial information, including databases, has been protected. It finally will offer some commentary for possible consideration about the rather unique approach to the protection of commercial data proposed and presented by the author's esteemed colleagues Professors Yang Jianzheng and Xu Chunming. Before undertaking this legal analysis, it maybe helpful first to examine briefly the key concepts that underlie information societies, databases and commercial information.

1. Information Societies

Consider first the term "information society." What are information societies? This is a phrase that is much used and that clearly can take on vast parameters in a construct

1 A copy of that presentation is attached hereto as Annex 1.
2 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of databases, OJ L 77/20 (27.3.1996).

such as the European Union's Information Society Directorate General.[3] At a very simplistic level, one might define an information society as one where the creation, use, distribution and reformulation of information underpin the economy as well as its social and cultural components.

In a UK report, labeled 'seminal',[4] the definition of an information society acknowledges a key component, technology, but as well its use in social contexts:

> Information Society: A society characterised by a high level of information intensity in the everyday life of most citizens, in most organisations and workplaces; by the use of common or compatible technology for a wide range of personal, social, educational and business activities, and by the ability to transmit, receive and exchange digital data rapidly between places irrespective of distance.'[5]

Thus, an information society also would encompass that policy surrounding the planning and of information economies, including its technological infrastructure, can as well focus on societal or social development. The risk of not having an adequate plan for both technology and its use in society was succinctly identified in this same report:

> All technology amplifies. Apparently indiscriminately, it amplifies efficiency or inefficiency, risk or caution, waste or saving, advantage or disadvantage. The more powerful the technology, the greater this effect is likely to be. When access to technology is linked to other social advantages such as wealth, education, and employment - as is usually the case at present - the risk of social exclusion will also be amplified.[6]

This understanding however was not novel in 1997 when this report was published. More than a decade earlier, there was extensive EU planning for the development of its 'Information Society' stated to further develop the Single Market as a competitive economic global player and to further its objectives of the advancement of the economic and social progress of its citizens. (Art. 3, EU Treaty). This planning which envisioned

---

3 This Directorate, now the Directorate General Information Society and Media, and its mission can be found at http://ec.europa.eu/information_society/index_en.htm.

4 The Net Result: Social Inclusion in the Information Society', Report of the National Working Party on Social Inclusion in the Information Society. (IBM Community Development Foundation 1997), available at: http://www.local-level.org.uk/uploads/Public_Documents/NetResult.pdf.

5 Ibid at 9.

6 Ibid. at 2.

greater social and economic inclusion encompassed: the physical infrastructure or networks and technologies as well as the telecommunications services necessary for the carriage, or exchange of information, [7] the content (digitized information of one kind or another)[8] and the commerce (including from the commoditization of information and services based on information) that would be provided over these networks.

Two of the EU's areas of focus included legal frameworks for the protection of databases and to enable electronic contracting, the topics addressed within the two days of this EU-China Information Society Project meetings and workshops. This report focuses on the first of these: the protection of a specific form of content, i.e., databases and the information contained within them. Returning to the examination of basic concepts, the following considers briefly 'What is a 'database'?'

2. Databases

A 'database' could be defined generally as an organized or structured assembly or collection of information, records or data to facilitate its access or retrieval. 'Data' is considered to be raw information used in context (e.g. reasoning, decision making, calculations, etc.). How the collection of data is structured and organized can vary according to its nature, use, how assembled (manually or by computer), etc. Thus, since everything about a database can vary, including the data, the structure and how it is used and assembled, it might be accurate to say that all databases are different.

Computer databases are those collections of data created by means of computer use management software to organize, maintain and access the data. There are different structures for the data according to the database model used, for example a relational database which structures each piece of data in tables comprised rows and columns according to categories. Each is assigned values according to rules and coded. A query to

7 Commission, Towards a Dynamic European Economy: Green Paper on the Development of the Common Market for Telecommunications Services and Equipment, (COM (87) 290 final, 30 June 1987).
8 Commission, Green Paper on Copyright and the Challenge of Technology: Copyright Issues Requiring Immediate Action, (COM (88) 172 final, 7 June 1988); Commission, Working programme of the Commission in the field of copyright and neighbouring rights: Follow-up to the Green Paper, (COM (90) 584 final, 17 January 1991).

the database for information matching the specific value will produce an output of data according to the requested categories.[9] There are other models.

a. The Directive's Definition The Database Directive has imposed a harmonized definition among its Member States.[10] It defines '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'(art. 1(2))

Other provisions of the Directive shape this definition. Thus, the definition does not encompass any software creation or management system (art. 1(3)), and hence within its protection. The Directive's definition also encompasses those manual databases meeting the above criteria. (Rec. 14) According to the Directive's Recitals[11] of the Directive, the term 'database' is otherwise to be understood to include:

- literary, artistic, musical or other collections of works

or

- collections of other material such as:
  - texts,
  - sound,
  - images,
  - numbers,
  - facts, and
  - data.

However, 'databases' does not extend to 'a recording or an audiovisual, cinematographic, literary or musical work as such'. (Recital 17). Further, compilations of recordings of musical performances on CDs are not considered to fall within the relevant definitions. (Recital 19). How the Directive protects such databases is examined subsequently.

[9] See 'XML: A Quick Relational Database Primer' (Brainbell.com Tutorials), available at: http://www.brainbell.com/tutorials/XML/A_Quick_Relational_Database_Primer.htm
[10] This of course is in the context of intellectual property protection.
[11] Recitals in EU legislation are statements of reasons for the legislation with non-mandatory language and that include both statements of relevant law and fact. Joint EU Guide for persons involved in the drafting of legislation within Community institutions, Recitals s. 10, available at: http://eur-lex.europa.eu/en/techleg/10.htm.

However, turning now to the last underlying concept, the next section considers 'commercial information'.

3. Commercial Information

The scope of this author's terms of reference for this research was an exploration of how commercial data is protected in the EU. The Database Directive is likely the primary if not the sole means whereby commercial data is protected on an EU-wide basis. The Directive does not itself, however, reference commercial data.[12] Databases within the Database Directive Databases can of course contain information that is 'commercial' within the broad definition above. Moreover, commercial data is a vast concept since any information could be considered 'commercial' once it is sought to be marketed as a commodity in the stream of commerce or relates to some aspect of commercial activities. This would include personal data sought and obtained by businesses for purposes of product development and marketing.

'Commercial data' can be divided into a number of categories that help organize it for purposes of this analysis: data generated by business operations (whether routinely or pursuant to an obligation such as a tax return); data used by businesses in their operations and; data or information that businesses seek to sell or otherwise exploit in the context of third-parties. One could label these: 'commercial operations data outputs', 'commercial operations data input' and 'commercial information products'.

Why should there be a focus on commercial information in particular? Clearly it is the potential economic value of this non-tangible asset. Although information's value is significantly correlated to how well it is organized, managed, and used, including as knowledge. According to one source, and using 'intellectual property' as a stand in for commercial information (although possibly under inclusive): 'If you look at the Fortune 500, the value of IP for its largest companies ranges between 45% - 75% and also

[12] The only use of 'commercial' in the Directive's provisions is those requiring that certain exceptions be applied for 'non-commercial' uses only. See arts. 6 and 9, 96/9/EC.

represents the highest growth area in the global economy.'[13] Another study values it as at least 20% of the market value of financial service organizations.[14] Another reason for the focus is information's use as an input to stimulate further the growth of information economies (or more value). It is because of this value or other societal values such as fairness and equity, that societies have accorded it varying degrees of protection.

Having now defined explored the terms: information society, databases and commercial data, this now examines how databases, including those that contain commercial data, are protected.

4. The EU Directive on the legal protection of databases

1. The Protection of Commercial Data within Databases

At the outset, it should be further emphasised that while the Directive on the legal protection of databases15 is likely the primary way that any commercial information contained within databases falling within its definitions as detailed above would be protected on an EU-wide basis pursuant to EU law, it is not the only way which commercial information is protected under the laws of individual EU Member States and other jurisdictions. Rather, commercial information can be protected under a range of other legal theories, including contract, the law of confidence, trade secret, unfair competition and unfair trade, misappropriation, copyright, 'catalogue' protection and criminal law. This report will briefly examine some of these legal schemes after considering the Directive and some issues surrounding its implementation.

2. Why the Database Directive?

In its planning process for the Directive, the Commission indicated the economic importance of commercial information that likely would comprise raw data that could be

[13] Cisco 'High Tech Policy: What is the Value of Intellectual Property?', available at: http://blogs.cisco.com/gov/comments/what_is_the_value_of_intellectual_property/.
[14] Hillard, R., McClowry, S., Na, L., 'Determining the Economic Value of Data for Financial Services Organisations' (2006) (Open Methodology) available at: http://mike2.openmethodology.org/wiki/Economic_Value_of_Information
[15] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (1996 OJL 77/20).

updated and manipulated. Noting in 1985, that databases contributed $5 billion dollars to the global economy of which 4/5 was attributable to the U.S., the EU considered that it needed to protect databases so that the EU could become more competitive in the information services market.[16] It also considered that the differing levels of intellectual property protection accorded by various Member States to databases created an impediment to the free flow of information goods and services thus undermining the development of the Internal Market that was at the very heart of the European Community. These differences largely resulted from the traditional schism in copyright protection between those EU countries where databases were not generally considered sufficiently 'creative' following the civil law 'author's rights' ('droit d'auteur') approach for protection of literary works in contrast to the common law of the UK and Ireland with its higher level of protection under the invested skill, judgment and labor approach that could more readily accommodate a collection of non-creative information. The result was a compromise between the two as well as a new and unique form of protection as is discussed in the following.

3. Overview of the Directive

The Directive protects qualifying databases in two ways: it harmonizes the level of protection for databases that comprise 'works' under copyright law and it creates a 'database right' to protect the investment in qualifying databases. This will examine each of these protections in turn.

A. Directive and Copyright

1. Protected databases

The Directive ensures that copyright protection for databases (as defined above) extends only to the "selection or arrangement of their contents", thus limiting the aspect of a database that is eligible for copyright protection not to any of the actual contents but how they are chosen and organized. This selection or arrangement, to be protected, must be the author's "own intellectual creation". The Directive stipulates that, other than this, "[n]o other criteria shall be applied" to determine eligibility for copyright protection of

[16] See Green Paper on Copyright, above n. 1 at s. 6.2.1.

databases in EU Member States. (Art. 3). Since the protection does not extend to the contents of the database, this makes it possible for a collection of non-protected works (such as public sector information where this is not copyright protected) to attract copyright in the work as a whole if what is in the database or how it is arranged meets the 'own intellectual creation' test.
This is a level of creativity requirement; a compromise between sweat of the brow under common law and the mark of the author's personality under civil law protection.

The test may be derived from Article V of the Berne Convention which protects 'collections of literary or artistic works such as encyclopaedias and anthologies which, by reason of the selection and arrangement of their contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections.' The items comprising the content of databases may not however be a literary or musical work. Berne, as well, does not encompass within its protections 'miscellaneous facts' with the character of press information.[17]

It has been suggested as well that the EU Directive's criteria for the copyright protection was inspired by the test promulgated under U.S. copyright law by the U.S. Supreme Court in *Feist Publications v Rural Telephone Service.*[18] This used very similar if not identical phrasing in its test for when collections of information could be protected under copyright. Even if it was not a direct source for the Directive, the case gives a good example of what might fall within and without its protection. In *Feist* a CD of telephone directories of phone numbers listed only in alphabetical order was found not to meet the test. Alphabetic order, the Court found, was an ordinary and totally objective criteria for the selection and arrangement of what were otherwise 'facts' unprotected by copyright. It was, therefore, insufficiently original to meet the test of a work of the author's own intellectual creation that is implicit in the U.S. Copyright Act.

To reach this conclusion, the Court first addressed the contents of the CD, which effectively comprised a database. The Court stated:

[17] See Berne Convention, art. 1(8).
[18] 499 U.S. 340 (1991), http://www.law.cornell.edu/copyright/cases/499_US_340.htm.

> It is this bedrock principle of copyright that mandates the law's seemingly disparate treatment of facts and factual compilations. "No one may claim originality as to facts." This is because facts do not owe their origin to an act of authorship. The distinction is one between creation and discovery: the first person to find and report a particular fact has not created the fact; he or she has merely discovered its existence. To borrow from *Burrow-Giles*, one who discovers a fact is not its "maker" or "originator." 111 U.S., at 58. "The discoverer merely finds and records." Census-takers, for example, do not "create" the population figures that emerge from their efforts; in a sense, they copy these figures from the world around them. Census data therefore do not trigger copyright because these data are not "original" in the constitutional sense. The same is true of all facts -- scientific, historical, biographical, and news of the day. "They may not be copyrighted and are part of the public domain available to every person." (Citations omitted).[19]

In contrast to the facts themselves, the Court considered that it would be possible for the selection and arrangement to meet the test of 'originality'. Here, the Court reasoned:

> Factual compilations, on the other hand, may possess the requisite originality. The compilation author typically chooses which facts to include, in what order to place them, and how to arrange the collected data so that they may be used effectively by readers. These choices as to selection and arrangement, so long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws. Thus, even a directory that contains absolutely no protectible written expression, only facts, meets the constitutional minimum for copyright protection if it features an original selection or arrangement.[20]

Unlike the mere alphabetical listing of the facts in the phone directory in *Feist,* however, in a subsequent case, *Key Publications v. Chinatown Today,* the court found that while alphabetical, the listing in a telephone yellow pages directory of businesses selected for their possible interest to the Chinese-American business community was sufficiently original to be protected under *Feist.*

The nature of the protection for original compilations of selected and arranged facts under *Feist* is noted to be somewhat limited since the facts themselves, likely in the public domain, are not protected. This according to the *Feist* Court, '*inevitably* means that the copyright in a factual compilation is thin. Notwithstanding a valid copyright, a

[19] Ibid. at 347.
[20] Ibid.

subsequent compiler remains free to use the facts contained in another's publication to aid in preparing a competing work, so long as the competing work does not feature the same selection and arrangement.' Thus, extensive copying or other prohibited act under copyright of the selection and arrangement of the facts (i.e., essentially the work as a whole) would likely be those from which the work is protected.

2. Nature of the Copyright Protections for Databases under the Directive

The exclusive rights accorded authors under copyright in the Directive refer to the right to prohibit acts in relation to the selection or arrangement of the contents. The acts are analogous to that for other protected works. Hence, the author has the sole right to do or authorize the following acts with respect to the selection and arrangement: (Art. 5):

- temporary or permanent reproduction by any means and in any form, in whole or in part;
- translation, adaptation, arrangement and any other alteration;
- any form of distribution to the public of the database or of copies thereof, subject to the exhaustion of rights;
- any communication, display or performance to the public;
- any reproduction, distribution, communication, display or performance to the public of a translation, adaptation, etc.

As noted by the Commission in its Proposal for a Directive on the legal protection of databases, the acts have to be done with a significantly sufficient portion of the database to constitute an infringement of rights in the selection or arrangement.[21] This is comparable to the reasoning in *Feist.*

3. Limitations on copyright protection

The Directive makes clear that this protection under copyright does not extend to the contents of the database. (Art. 3(2)). Also, a lawful user of the database is not precluded from doing any of the above acts in order to access or use the database lawfully, or that part for which the lawful user has authorization. (Art. 6(1). This was considered necessary for lawful users to be able to exercise their contractual rights since the access of the database could involve the reproduction of the entire selection and arrangement,

[21] See ibid. at s. 5.0, available at: http://aei.pitt.edu/8653/01/31735055263457_1.pdf. (Attached as Annex 2).

such as with the booting up of a database on a CD or a temporary copy of a database that would be created in RAM in accessing an online database, although it is not clear that this would necessarily be sufficiently significant and would turn on how much was accessed. Beyond the lawful user exception Member States also had the option to allow any or all of the following limitations to the right of the author as well as any traditional limitations to copyright: (Art. 6(2)

- reproduction for private purposes of a non-electronic database;
- use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;
- use for the purposes of public security of for the purposes of an administrative or judicial procedure.

B. The Sui Generis or 'Database' Right

The sui generis database right is intended to protect the 'maker's' 'substantial investment' determined qualitatively and/or quantitatively in either the obtaining, verification or presentation of the contents of a database (as previously defined). It protects the maker of the database (i.e., the one who takes the risk of this investment) from unlawful extraction of the whole or substantial parts of the contents of the database and their subsequent re-utilization. The substantial investment needed to qualify a database (still meeting the original definition) for the sui generis right need not be merely financial, however. [22] It can extend to labor and time and other resources. The sui generis right applies whether or not the database meets the criteria for copyright protection. (Art. 7(1)).

The unauthorized extraction and/or re-utilization of the whole or of a substantial part is to be evaluated qualitatively and/or quantitatively. (Art. 7(1)). 'Extraction' includes the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form. (Art. 7(2)(a)) 'Re-utilization` means any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of

[22] This has been the subject of interpretation by the European Court of Justice in Case C-203/02, *The British Horseracing Board Ltd and Others v The William Hill Organization Ltd* [2004], discussed infra at 21.

transmission. (Art. 7(2)(b)). Upon the first sale of a copy of the database, this right of reutilization is extinguished with respect to that copy within the EC. Neither the right of reutilization or extraction includes public lending.

1. Limitations on the sui generis rights

Lawful users of a database that is made available to the public may freely extract and/or re-use **insubstantial** parts of the database. What comprises an insubstantial part under what the Commission has described as a compulsory license to the lawful user[23] is also evaluated both qualitatively and quantitatively. The database rights holder cannot restrict how these insubstantial parts are used. (Art. 8(1)) However, lawful users, may not "perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database," (analogous to the art. 9(2) Berne three-part test) nor prejudice copyright or related rights (if any) in the works that are the content of the database. (Art. 8 (2)) The Directive allows Member States to provide the following exemptions/limitations to the database right analogous to those under copyright: (Art. 9)

- in the case of extraction for private purposes of the contents of a non-electronic database;
- in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;
- in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure.

2. Term of protection

An interesting aspect of the Directive's sui generis protections arises with respect to its term of protection. While this is 15 years, (art. 10(1)), a new substantial investment in updating and changing it will qualify the database that results for its own full term of protection. Thus, it is possible that there could be a continuous, rolling term of 15 years of protection as long as this updating is done. In this regard, the Directive requires:

> Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the

[23] See Explanatory Memorandum, Commission Proposal for a Directive on the legal protection of databases, above n. 20.

accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively. (Art 10(3)).

3. Reciprocity Limitation

The beneficiary of the database right is limited to databases whose rights holders ('makers') are either: 1. EU nationals or persons having their habitual residence in the European Community or 2. companies and firms formed under the laws of Member States and having their principle place of business or registered office in the Community. Where the entity has only a registered office, its operations must have a substantial link to the economy of a Member State.

The Directive requires that third countries offer reciprocal protection pursuant to treaty in order for it to extend the database right to databases made in third countries whose right holders/makers don't fall within the above categories. (Art. 11)

4. Evaluation of the EU Directive on the legal protection of databases

This section intends to provide a brief overview of some of the issues and concerns that its adoption has raised. The Database Directive has always had detractors. While some questioned whether the protection was sufficient,[24] many other commentators found it over protective, notably from the academic and scientific and library communities.[25] They raised significant issues including the concerns that the sui generis right was an over-protection that could result in public domain information being locked up in exclusive-source databases.[26] Sole source databases could produce monopoly pricing. Commentators also noted that access to data as a basic building block of research would become more costly and difficult in light of the growing and extensive commercialization of electronic publishing and electronic databases in which papers promulgating the

[24] See, e.g., DG Internal Market, Working Paper: First Evaluation of Directive 96/9/EC on the legal protection of databases (12/12.2005) at 4, available at: http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf. (Attached here as Annex 3).

[25] See D. Greenbaum, 'Are We Legislating Away Our Scientific Future?': The Database Debate' 2003 DUKE TECH. L. REV. 22

[26] See C. Colston, 'Sui Generis Database Right: Ripe for Review?, 3 J. Info. L. & Tech. 4, §§ 2.2, 3.2 (2001), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/colston.

results of research that is often government funded are now routinely published.[27] The Directive does not have a compulsory licensing scheme that might address these concerns although one was dropped from an earlier version. Others have noted that this would prove cumbersome and that where both copyright and database protections existed, the licensing and assignment would be legally complex.[28]

Other concerns arise concerning research and its publication. Researchers often extract information from earlier papers to be reused within their own research that is then published by another commercial publisher. The second generation publisher could be risk for this publication not being able to anticipate if this extraction comprises a substantial part qualitatively and quantitatively to the first publisher. Unlike the researcher, the second publisher has a commercial purpose. Even the original researcher may have concerns that inhibit use since the research limitation, akin to a fair use doctrine, since what can prejudice the legitimate interests and conflict with normal exploitation may not be clear as well. Others have questioned the value of this protection in light of the growing costs of access to information input needed by businesses as a result of the protection.[29]

The Directive does not have a definition of 'value added' which would help limit the protection to the maker's efforts in connection with information that could otherwise be in the public domain such as government published information or other publicly available information.

These negative consequences would likely be justified if the balancing exercise that is involved in according any exclusivity or restrictions on the rights of others involved in IP protection achieves its intended results. Here that was to establish a harmonized protection including the sui generis right in order to promote the development of EU

[27] See, e.g., "The Trend Toward Strengthened Intellectual Property Rights: A Potential Threat to Public-Good Uses of Scientific Data" in 'Bits of power: Issues in Global Access to Scientific Data, Committee on Issues of Transborder Flow of Scientific Data' at 134, U.S. National Committee of CODATA, National Research Council (National Academy Press 1997).
[28] S. Gosnell, 'Database Protection Down Under: Would a 'Sweaty' Australia Be Better Off With A Northerly Change?'[2003] UNSWLJ 43, http://www.austlii.edu.au/au/journals/UNSWLJ/2003/43.html.
[29] See J. Hladjk, 'The protection of databases under EU and US law-the sui generis concept as an appropriate concept? [2004] Comp. L. & Sec. R., 20:5, pp. 377-383.

origin electronic databases.[30] On this aspect, however, the most damning evaluation of the Directive comes recently from the EU itself. As the Commission noted in 2005, nearly 10 years since the Directive's promulgation, pursuant to an empirical study, the Directive has not proven successful in meeting its economic objectives. Based on the lack of growth of the EU database industry as measured by the pre-Directive level of European origin databases despite the Directive's implementation, the Commission whether it had continuing justification.[31] Despite the economic evidence, it seems the rationale may exist primarily in the form of claims by database makers to feel well protected and that the Directive is 'essential' to their continued operations. One must question this as a basis for continuing a legal regime as it would be difficult to find many intellectual property rights holders willing to relinquish rights, outside of the creative commons groups who tend to be computer engineers and other academics and scientists, etc., concerned about the ability to build on prior knowledge.[32] Another finding that must be considered is that while the rationale for implementing its sui generis protection was the EU's targeted objective of becoming more competitive with the U.S. in its database creation, the U.S. has had continued growth despite that it still does not protect compilations of fact, as discussed above.

There are reasons which the Commission has attributed as contributing to the Directive's weaknesses, including the differing implementations in the Member States and that the significant terms do not have traditional accepted meanings. Thus, its construction by the courts in the Member States and the ECJ is the plowing of new fields. It has further been suggested that a number of key decisions have substantially weakened the Directive from its original intent. Perhaps key here is the ECJ decision in *The British Horseracing Board*

[30] See Introduction, Explanatory Memorandum, Commission Proposal for a Council Directive on the legal protection of databases. Accord, Working Paper 'First Evaluation of Directive 96/9/EC on the legal protection of databases' (DG Internal Market 12/12/2005), pp. 3-4.
[31] See generally Working Paper 'First Evaluation of Directive 96/9/EC on the legal protection of databases' (DG Internal Market 12 December 2005).
[32] Indeed, this approach by the Commission has been criticized as an adherence to its 'faith-based policies' and 'voodoo economics' and analogized to asking farmers or monopolists if they liked their subsidies and economic power. See J. Boyle, 'Two database cheers for the EU' (FT.com January 2, 2006), available at: http://www.ft.com/cms/s/2/99610a50-7bb2-11da-ab8e-0000779e2340.html.

v William B. Hill.[33] Here the ECJ ruled essentially that there is a distinction between *creating* new data for purposes of the meeting the substantial investment required for the database right and the *obtaining* and *verifying* the data in its entry as contents of the database. Thus, the lists of horses, races, jockeys, etc. that the BHB created for another purpose, i.e., performing its oversight of racing functions, could not be credited toward the substantial investment in obtaining/verifying the contents of the database. BHB licensed commercially that primarily comprised this information. Other ECJ cases have in other ways limited the scope of the Directive.[34]

In light of the fact that the Directive has perhaps not proved an optimal form of protection, it may prove helpful to consider what other legal regimes are used to protect commercial data. The following section does this.

5. Other Regimes for Protecting Commercial Data

Commercial data can be protected using various legal theories in many jurisdictions. These include contract, tort, equity, such as confidence, competition/unfair trade, computer crime, and certain forms of IP such as the Nordic 'catalogue' protection. There are jurisdictions, however, where the law fails to recognize a quantifiable harm in the taking of mere information which has no perceived inherent value unlike other intangible properties. The following provides an overview of the most significant of these legal regimes, including a discussion of their perceived weaknesses in protecting commercial data.

In addition to the legal protections, one cannot disregard the technological protections. With growing ability to apply access and use controls to electronic works, these present a significant measure of database content protection.

1. Law of confidence

In the UK, theft of commercial (and other) information is not protected unless the information in question has been provided in confidence either explicitly pursuant to

33 Case C-203/02, The British Horseracing Board Ltd and Others v The William Hill Organization Ltd [2004].
34 Discussions of these cases are attached here as Annex 4.

agreement or implicitly arising from the nature of the information, the relationship and the circumstances. Here, the law of confidence, pursuant to the holding in *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41, will protect such information and provide a remedy to the confiding party in the form of damages or an injunction to prevent or delay its disclosure (to take away any market advantage the breach may provide) if the following criteria are met:

- the information (of whatever kind: trade and business secrets, personal information, etc.) in question has the necessary 'quality of confidence' (it has been protected and not disclosed routinely);
- the party to whom it was entrusted had a duty to keep it confidential (arising from contract, relationship, explicit request, professional status (e.g., doctor) or under otherwise obvious circumstances) and;
- there is or likely to be an unauthorized disclosure of the information to the harm of the confiding party.

The doctrine is to some extent based on principles of equity[35]and will therefore seek first to prevent the information's use or release and restore the parties to their prior position. Damages are possible as well.

Canada has recently used the theory of a constructive trust in the context of confidence which avoids the need to establish clearly the precise underlying legal theory justifying the protection (equity, contract, or property law), thus creating some greater flexibilities in confidence as a remedy. As noted '[t]he action is *sui generis* relying on all three to enforce the policy of the law that confidences be respected...'.[36]

In the context of databases and their protection under the law of confidence, the Canadian government has identified the following issues:

> The breach of confidence proceeding is important to this study (of database protection) for two principal reasons:
>
> > (a) A database or compilation may be protected as confidential information or a trade secret. The difficulty, however, is that most databases are designed to be accessed, often by the public, even if on payment of a fee. This will ordinarily mean, at least with respect to the

[35] But has been premised under implied or explicit contract and on property interests (e.g., *Albert v Strange* where Prince Albert's personal drawings were threatened with publication in a catalog)
[36] *LAC Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574. 615 (Spinka, J.).

> subject matter or content of the database that it cannot possess the necessary "quality of confidence". However, a database may present:
>
> (i) sufficient secrecy or "quality of confidence" in a particular method of selection or arrangement of the database. This need not be "novel", in a patent sense of that expression, but it would need to be not generally known. In this sense the position would be similar to the Feist test for originality in copyright. Courts in the United States have protected computer programs as trade secrets on this basis; and
>
> (ii) a collection of subject matter known to the public, and therefore not secret, but nevertheless saving a subsequent compiler from going to the trouble of collecting the information independently. The later compiler has been given an advantage. This has been termed the "springboard principle" and has been described as remaining "even when all the features have been published or can be ascertained by actual inspection by any member of the public". Similarly, the information may be only partially known to the public, but brought more fully into focus by additional non-public information.[37]

In light of the above, this Copyright Policy Office report on Canadian database protection concluded that while this theory can provide a measure of protection to databases, it does have limits to its applicability. As it concluded confidence's 'principal limiting features' are:

> (a) The need to predicate protection and liability upon the quality of secrecy or confidentiality, even when broadened to what has been described as "relative" secrecy; and
>
> (b) The formulation of the proceeding that requires that the information be imparted by the holder (the confider) to another (the confidee or confidant) before a "relationship" of confidence is established. Essentially, this limits the scope of the proceeding to a breach by a person who has had the information imparted to him or her:
>
> (i) In a contract stipulating non-disclosure of the information; or
>
> (ii) In circumstances that reasonably imply an obligation of confidentiality'.[38]

Since often a database will be published, it is unlikely to have the quality of confidence outside a contractual limitation requiring its contents to be kept confidential. Here as

[37] Canadian Heritage, Copyright Policy Branch 'Database Protection in Canada: Trade Secret/Confidential Information – The Relevance of Breach of Confidence to Databases', § 2 (a), (Ottowa 17/02/2003) available at: http://www.canadianheritage.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/database/18_e.cfm.
[38] Ibid. at § 2 (b).

well, the efforts to maintain its confidentiality would be relative to the quality of confidence would be relevant. The broader the subscription base, the less likely it will meet these criteria.

2. Trade Secret Law

Trade secrets in the UK would fall under the law of confidence. This would be just another form of confidential information. In the U.S., however, numerous states follow what is called the Uniform Trade Secret Act (UTSA), a model law. The UTSA provides that for misappropriation of trade secrets, a claimant can obtain damages as well as injunctive relief (to prevent its use or disclosure). The model law defines 'trade secrets' as:

> 'information, including a formula, pattern, compilation, program device, method, technique, or process, that:
>
> > (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> >
> > (ii) is the subject of efforts that are reasonable under the circumstances *to* maintain its secrecy.'

This is a very broad definition of a trade secret that could encompass a database and its contents. As the latter part of the definition of a trade secret is a test for the quality of confidence somewhat comparable to UK law, similar limitations to those noted above, however, would apply.

The model law defines "misappropriation" as the acquisition of another's trade secret by one who knows or should know it was acquired by improper means or its use or disclosure without express or implied consent and by a person who:

> (A) used improper means to acquire knowledge of the trade secret; <u>or</u>
>
> (B) at the time of disclosure or use knew or had reason to know that knowledge of the trade secret was:
>
> > (1) derived via a person who used improper means to acquire it;
> >
> > (2) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; <u>or</u>

> (3) derived via a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (4) before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

Improper means here includes "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means."

Not every U.S. state follows this broad definition of trade secret, however. Some adhere to the more restrictive definition under the Restatement (3rd) of Unfair Competition Law that requires an actual competitive disadvantage to be proved. That might seem to require that the information extracted from a published database to be incorporated into another that competes with the first.

3. Contract

Contract law can be used to protect commercial information. Examples include confidentiality agreements or licensing restrictions regarding access to and use of information (e.g. 'know how'). The latter could extend to information in databases. Even a 'click through' license ("I agree") for an online database will generally be found enforceable. As noted by the U.S. Copyright Office:

> [T]he core coverage of database contracts tends to be similar: contracts restrict access, specify permissible conditions of use, and set terms for enforcement and remedies. They may also contain language designed to educate the consumer about legal rights and limitations.
>
> For databases other than those made freely available to the public (such as telephone directories), contracts are generally the condition of access for a user. Even for a noncopyrightable database, they can also offer users the benefit of timely, updated information.
>
> One common use of contracts is to restrict or limit the manner of use of a database. An on-line license typically dictates the parameters of acceptable downloading and redissemination… .[39]

[39] U.S. Copyright Office, Report on Legal Protection of Databases (Washington 1997),available at: http://www.copyright.gov/reports/dbase.html See the text of this Report for a further discussion of contractual provisions.

The biggest limitation of contract is that it will not bind non-parties (e.g., non-subscribers) to an agreement which may be only the first purchaser of information on a CD. Enforcement in an online environment may as well prove difficult given the usual issues of geographical diversity, costs, locating the infringing party, etc. These however are not issues unique to databases and large content owners have not been deterred generally.

4. Criminal Law

Criminal laws can be effective sources of protection for commercial information. While general theft laws may require property or property of a certain value to have been stolen, in some jurisdictions information does not comprise property or does not have an inherent value. However, computer crime laws may apply where a computer holds the information. For example, the UK Computer Misuse Act may encompass the entry without authorization into a computer-operated database, whether online or not. The extraction of data may well fall within its other prohibited acts. In another example, § 1030(a)(2) of U.S. Computer Fraud and Abuse Act[40] makes it illegal for anyone to access without authorization a protected computer (connected to the Internet, among other things) and obtain information if an interstate or foreign communication is involved. This would encompass information obtained using the Internet from an online database. Such statutes may apply damage thresholds below which they may not be applicable. If information does not have an inherent value in a jurisdiction this may prove a barrier. The above statute however has no such applicable provision. It permits civil actions.

Also in the United States, the Economic Espionage Act 1996 criminalizes the 'theft of trade secrets'. (18 U.S.C.A. 1832). This, however, while protecting

> "all forms and types of financial, business, scientific, technical, economic, or engineering information ... whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."

still requires, as with civil forms of trade secret, that it have the quality of confidential information, including an independent economic value from being kept secret.

[40] 18 U.S.C. § 1030 (a)(2).

5. Unfair Competition

Unfair competition primarily concerns torts that cause an economic injury to business by means of a deceptive or wrongful business practice.[41] The nature of unfair competition varies and under both civil[42] and common law can include such things as trademark infringement, misappropriation of intangible assets not protected by trademark or copyright, use of confidential information by a former employee to solicit customers, theft of trade secrets, etc. The laws of numerous countries protect the misappropriation of commercial information as unfair competition. This unfair competition can be based on varying legal foundations, including a free rider unfair advantage theory (e.g., in France '*concurrence parasitaire*')[43]. This can entail profiting from another's achievement to exploit its clientele at the other's expense which can clearly encompass a theft and reuse of commercial data. In the United States, misappropriation as unfair competition has been noted to be a tort that originates from a 1918 U.S. Supreme Court decision, *International News Service v. Associated Press.*[44] Here one news agency took the news from the east coast early editions of papers printed by the members of the other association. Using these uncopyrightable facts, it rewrote the stories and sent them to its west coast member newspapers taking advantage of a 3-hour time difference. The Supreme Court found that the defendant had misappropriated the 'hot' news of the other agency giving it an unfair competitive advantage. In reaching this conclusion, the Court found that the claimant had obtained an intangible quasi-property interest in the news while it was fresh or 'hot'.[45]

Due to limitations on U.S. federal courts creating federal tort law and its possible pre-emption by copyright law,[46] many courts applying *INS* have limited it narrowly, for example to facts where:

---

[41] See 'Unfair Competition Law: An Overview', Legal Information Institute (Cornell University Law School, available at: http://topics.law.cornell.edu/wex/Unfair_competition.
[42] See generally, A.K. Sanders, Unfair Competition Law: The Protection of Intellectual and Industrial Creativity (OUP 1997).
[43] See ibid. at 25.
[44] 248 U.S. 215 (1918).
[45] Ibid. at 219-221.
[46] It has been noted that unfair competition theories in countries beyond the U.S. can also be subject to pre-emption based on intellectual property laws such as trade mark statutes. See A.K. Sanders, above, note 40 at 6-52.

- The claimant generates or gathers information at a cost;
- The information's value is that it is time sensitive
- The defendant's use is free riding on the labor of the claimant
- It is in direct competition with the claimant's products/services
- The ability of other parties to free-ride on the efforts of the claimant would significantly reduce the incentive to produce the product or service that its existence or quality would be substantially threatened because the cost would be so prohibitive when compared to the return.[47]

The application of these requirements is not uniform, however. Other U.S. courts have required only an economic harm.

The limitations of unfair competition are that the taking and use of the commercial information would have to be in the context of trade and with a resulting economic harm or competitive disadvantage. These are however perceived to be its advantages over another more extensive form of protection like the *sui generis* right as this is a very likely scenario for theft of databases and other formats of commercial information and allows the claimant to proceed against a competitor where there is economic damage. It is further considered not to enhance the already significant market power of sole source database owners and preferable to an inadequately balanced set of sui generis rights and limitations for purposes of scientific and other innovation.[48] Other non-competing uses of the information would not fall under this theory.

6. Copyright and Compilations

Where the commercial information has original expression, that expression is of course protected by copyright. The ideas or facts are not themselves protected and can be used by others. This is the traditional idea/expression dichotomy of copyright. Because the term is so long, it is only that original expression that is protected in order to reward the author's efforts and to encourage works to be published and ultimately enter the public commons.

---

[47] *NBA v. Motorola*, 105 F.3d 841 (2d Cir. 1997).

[48] See, e.g., "The Trend Toward Strengthened Intellectual Property Rights: A Potential Threat to Public-Good Uses of Scientific Data" in 'Bits of power: Issues in Global Access to Scientific Data, Committee on Issues of Transborder Flow of Scientific Data' at 164, U.S. National Committee of CODATA, National Research Council (National Academy Press 1997).

Compilations of otherwise unprotected pieces of information may be protected separately from literary works under copyright. The UK for example still protects compilations where there is skill, judgment and labour used in compiling its contents. This is a lesser test than *Feist* and of the Database Directive. Therefore, collections of information such as directories would be protected as long as they were original (in the sense of not copied) and evidenced sufficient skill, judgment and labour. Trite, commonplace assemblies of facts such as those found in the fronts of pocket dictionaries (e.g., tables of standard weights and measures) do not qualify. This would protect commercial information assembled into a compilation and therefore databases. Although it is to be questioned whether this is a violation of EU law since the UK has not really harmonized its protection of these. However, it can be seen as one workable approach to the protection of commercial information which has limited ways of being expressed. This is the approach used in Australia and other common law jurisdictions that followed the UK law prior to the Directive although some of the cases make a distinction between the unprotectable mere 'industrious collection' and the requisite 'skill, judgment and labour' in compiling the information, etc.[49]

While catalogues of information can be protected as 'compilations' under these common law jurisdictions, in certain civil law countries, there is a separate or sui generis intellectual property protection of 'catalogues'. This is a form of 'thin' IP protection given to non-creative collections such as catalogues would be. The term of protection is usually short and requires nearly virtual copying, such as website scraping in an online environment. As noted by WIPO, such laws have been used for the protection of non-original 'databases' as follows:

> The subject matter of the protection is indicated in the laws of *Denmark* and *Sweden* as "catalogues, tables and similar makes in which a great number of items of information have been compiled." The provisions in the laws of *Finland* and *Norway* are almost identical, but they add "programs" (meaning exhibition programs and the like, in *Denmark* and *Sweden* that word was deleted from the laws to avoid confusion with computer programs) and the Law of *Norway* also adds "formularis." The Law of *Iceland* is broader in that it covers "a published writing" to which

[49] See, e.g., J.Lambert, 'Case Note: Desktop Marketing Systems Pty v Telstra Corporation Limited' (NIPC IP/IT Update Nov. 2002), http://www.ipit-update.com/copy33.htm.

> copyright does not apply. Thereby, that Law also distinguishes itself from the other Nordic laws in that its scope of protection is limited to subject matter which is not subject to copyright protection. The corresponding provisions in the other Nordic laws expressly state that concurrent copyright protection (and, in the Law of *Denmark*, also any other protection) may be invoked. These laws do not establish any criteria of originality or the like, apart from the demand that a large number of items of information must have been compiled. This means that individual data and insignificant compilations do not enjoy protection. The Law of *Iceland* does not limit its application to collections, but it may be assumed that the expression "a published writing" also excludes protection of individual data.
>
> The protection granted under the Nordic laws cover copying (in Iceland, reprint and copying) only. No protection is granted against other use, and the laws do not specify to which extent they are applicable as regards unauthorized extraction and copying of parts of protected compilations.[50]

These laws protect the catalogues as productions requiring significant financial investments and effort.[51] This is similar to the approach of the sui generis protection under the Database Directive which arguably is loosely modeled on these. As these laws generally protect from nearly wholesale copying, however, they would not protect individual information as could the Directive's sui generis right. Their typically short term (5-10 years) is still relatively long (in contrast for example to 'hot' news) but still shorter than the 15-year term of protection under the EU sui generis protection for databases.

7. Technological

A final category of protection for commercial information that cannot be dismissed is technological protection measures to control access to, transfer of as well as use of the content of electronic content. These have the ability to enforce established pre-established limitation and can be used in addition to the other forms of protection. These can include such technologies as PINs, time-limited registration keys, encryption, activation codes, digital watermarking, download and copying limitations. These measures are still

[50] WIPO, Memorandum: Existing National and Regional Legislation Concerning Intellectual Property in Databases (Geneva 30/06/1997), http://www.wipo.int/documents/en/meetings/infdat97/db_im_2.htm.
[51] CODATA, Bits of Power, above note 27 at 146.

evolving, often in response to the ability of others to bypass them. A further limitation is that they cannot protect access to printed databases and commercial information.

II. Conclusion

There are a numerous legal regimes for protecting commercial information, including that contained in assemblies or compilations that may be labeled ‘databases’. The EU regime is perhaps the most protective of non-original databases although now that the ECJ case law has raised the burden for substantial investment test for protected databases, the UK (and other common law jurisdictions’) compilation protection may offer broader protection. Some jurisdictions offer layers of legal protection via contract, tort as well as intellectual property protection.

The balance that is set between protection of ‘commercial’ information in order to promote innovation and economic development and over-protection which can undermine access to knowledge and second-generation, value-added uses of such information is a difficult one. In contemplating any new regime that seeks to protect commercial information, China may find it helpful to consider the experience of the EU with its Directive on the legal protection of databases from its own assessment and that of other commentators as discussed above and further detailed in the cited publications.

For many commentators, unfair competition is considered the form of protection which achieves this balance for commercial information as unfair competition would only protect information in which the claimant had an economic investment and which misappropriation would cause a competitive harm essentially requiring its use by competitor for actionability.

The model that has been proposed by the author’s esteemed colleague Professor Jianzheng Yang moves away from existing models. It appears to contemplate a sui generis form of protection analogous to that implemented in other jurisdictions for the protection of personal data: a commercial data protection regime. Having only reviewed the outline presentation of Professors Yang and without access to the full draft, any comments must necessarily be limited. It is hoped the following are received as intended: possibly helpful suggestions for further evaluation in subsequent drafting.

Firstly, it must be said that this is an innovative approach. While there are a limited number of EU (Austria and Italy, for example) and other countries (e.g., Switzerland) that protect legal persons under their data protection laws, this protection generally contemplates the collection, storage and use of data that 'relates' to or concerns the corporation/partnership/association. It does not encompass any and all data held by the legal person as appears contemplated by the new proposal. These countries' extension of data protection for the processing of appears premised on considerations with foundations in human rights theory that legal persons can have interests similar to individuals in finding out what information held about them by others is used to take significant decisions, e.g., such as to their creditworthiness, and to ensure the accuracy, relevance and currency of the data in that context. Information about small businesses and associations may largely comprise personal data, so that the boundary between personal and non may be blurred while the same compelling interests of fairness and control over information about the person may exist despite the legal form.

In light of its scope and scale, the government must of course evaluate its feasibility from the point of enforcement, compliance and likely effectiveness. Some concerns are presented which may of course be addressed by further detail. The following presents both these and benefits of the proposed ideas in no specific order:

- The proposal apparently contemplates a full regulatory regime that will require oversight by a national commercial data protection authority (akin to the DPAs that exist in the EU under 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). This is a vast undertaking and will involve considerable cost and human resources on the part of the government.
- It takes a public law, ex ante, and possibly one size fits all information approach to protecting private commercial data over the more traditional private law schemes (contract, tort, copyright, etc.) that rely for the most part on individual to utilize protections of any rights in the commercial data (e.g., via licenses, assignments, confidentiality agreements, employment contracts, assertion of

copyright) and enforce them when it is of enough value or import to justify this enforcement.

- Whether this is appropriate and necessary might be evaluated in the context of whether there is an appropriate legal infrastructure to enforce rights via private law. It might also be considered whether this public law framework will ultimately be a layer over private law as will not enterprises be likely to use private enforcement mechanisms to seek private damages.
- The determination of when a violation of the regulation has been committed may involve extensive ad hoc decision making on the part of the regulator. The desirability of this might be considered in contrast to decision making by the courts that are developing expertise and a body of jurisprudence in intellectual property as well as other private law actions. Whether there could be the possibility of conflicting decisions under both the public and private law regimes might be evaluated.
- All forms of regulation involve a cost to the regulated. Whether the benefit of the regulation outweighs its cost is one of the key factors for evaluating whether a proposed regulation is efficient and effective. The costs of compliance might take many forms, including delays or inability to use information where the 'owner' cannot be found and permissions obtained, the need to build systems for online compliance, etc. The EU data protection has been criticized including by a number of its Member States as unduly burdensome and difficult, creating great legal uncertainty and imposing vast costs including fees to legal advisors. The need for the public law approach taken here with personal data must be contrasted with what might be necessary for commercial data as with personal information there is often no alternative means of enforcement since it is not considered to have inherent value and damages are difficult to establish arising merely from the taking or disclosure of personal information even where there is personal humiliation. Examination of the EU experience including those countries that have protected the 'personal data' of legal persons may provide

some insights into the issues involved establishing the necessary infrastructure to implement and enforce these broader protections.

- The proposed legislation would appear to create rights in those who collect or generate commercial data legally. It is possible to collect vast amounts of data from publicly available sources: government directories, websites, census data, etc. How would the right owner, a second generation user of such information now collected into what may be considered 'commercial data' be able to enforce its rights against another party who collected the same publicly available information? At what point does the act of collecting amount to a propertization in the information?
- The definition, therefore, of what comprises 'commercial data' would be of critical importance to the feasibility of the proposed regulation.
- The information security obligations are also innovative. To date the primary information security obligations imposed on businesses have arisen in the context of personal data, including the Data Protection Directive or the U.S. Health Insurance Portability and Accountability Act's extensive security obligations for 'protected' health data. The Sarbanes-Oxley Act requires CEO's and CFO's to be able to swear under threat of criminal sanction that the data represented in their reports and the information on which it is based has integrity (not tampered with), thus entailing a significant corporate information security obligation that has extraterritorial effect as it applies to U.S. listed companies and their subsidiaries and affiliates. This has been identified has having very extensive compliance costs.
- It is not clear whether the proposal's obligation extends beyond the requirement to back up information. If so, while a worthy objective, it would merely allow continuing access by the enterprise to information. It would not necessarily ensure the integrity of the commercial information or its value to others for re-use.

- The need for computer security measure appropriate to the nature of the information might be considered. For example, the threat to personal data has been identified by a significant percentage of the population in developed countries (40-70%) as a serious deterrent to their use of the Internet for commercial transactions. Both e commerce and e government can be retarded in their growth and take up if such concerns were to trend out in China. The legal literature has begun to identify expressed concerns by Chinese middle classes as to the safety of their personal data.

- The draft proposal seems to include personal data within the definition of commercial data. This would seem appropriate as personal data is reported to comprise at least 5% of all commercial data. Here as well more than data back up would seem appropriate in light of the potentially serious economic harm that can result to an enterprise for failure to secure personal data appropriately. Studies by Professors Gordon and Loeb, University of Maryland Robert A. Smith School of Business, in a series of studies have sought to quantify the economic impact of computer security breaches. They have identified a 5% loss in share value enduring at least for 2 years for listed companies reporting computer breaches involving breaches of confidential personal information.[52] This is in addition to any direct costs to the company from the breach, including damages or administrative penalties.

- Much commercial data takes place in international data flows. Therefore, the application to and enforcement of this regime across international would seem a difficult issue that should be carefully considered.

[52] See Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou, 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market' Journal of Computer Security 11 (2003) 431-48 (IOS Press); Lawrence A. Gordon and Robert Richardson, 'The Economics of Information Security' Network Computing (1 April 2004)(' a leak of confidential information--an attacker spewing a bank's customer data across the Internet--could destroy customer confidence and create potential for lost revenue, causing the company's market value to plummet. In fact, companies that suffer a confidentiality violation lose more than 5 percent of their market value, on average, according to our research.'),< http://www.networkcomputing.com/showitem.jhtml?queryText=&articleID=18402774&pgno=3>.

- Open exchange of data in international scientific and academic communities is a positive value. With much of this information now being digitally managed and transmitted, there might be a need to consider how this exchange would be impeded by requirements of the proposed regulation. Here as well, identified concerns of possession or collection giving rise to property interests in the data may apply.

November 11, 2008

III. Annexes

I. Anne Flanagan, Presentation Slides, Commercial Data and Information Societies.

II. Commission Proposal for a Council Directive on the legal protection of databases (COM 92/24 final) (Brussels 13 May 1992).

III. Working Paper, First Evaluation of Directive 96/9/EC on the legal protection of databases (DG Internal Market and Service Brussels 12 December 2005).