Bloomberg
CORPORATE LAW JOURNAL

Volume 3 Spring 2008 Issue 2

Database M&A - What's Different?

Jeffrey C. Johnson, Steven J. Pierce and David E. Parsly
Pryor Cashman LLP

Reprinted from
Bloomberg
CORPORATE LAW JOURNAL
Volume 3, Spring 2008, Issue 2

ELECTRONIC DATABASES

DATABASE M&A - WHAT'S DIFFERENT?

By Jeffrey C. Johnson, Steven J. Pierce** and David E. Parsly****

INTRODUCTION

In modern society, as electronic databases continue to grow in size, complexity, and sophistication, databases have emerged as a highly valuable asset for many companies. Indeed, the information contained within a database, and the database's ability to manipulate that information in specific ways, can make each database a desirable commodity in a variety of commercial applications. With increasing frequency, databases are becoming a primary target of many merger and acquisition transactions. This article will explore legal issues that are particularly critical, and in some cases unique, to the purchase and sale of database assets.

What Is a Database?

As a preliminary matter, it is important to consider what exactly constitutes a database. A database is simply a collection of information organized in a way that is accessible, and can be something as large and sophisticated as *Lexis*® or *Westlaw*® or as simple and mundane (by today's standards) as a Rolodex®. However, the focus of this article is electronic

* *Jeffrey C. Johnson is a partner in the New York office of Pryor Cashman LLP. He specializes in the transactional aspects of technology and intellectual property exploitation. In particular, he has significant experience in all aspects of mergers and acquisitions, joint ventures, strategic alliances, private placements and licenses in the biotech, entertainment, Internet, pharmaceutical, software and telecommunications industries. He has been an invited speaker and panelist at a variety of public and private events, including the Digital Commerce Summit in 2006. Mr. Johnson is a co-author of the U.S. Law chapter of the World Online Business Law Digest, and is also a co-author of* Health Insurance Portability and Accountability Act-Compliant Merger and Acquisition Transactions, *2* BLOOMBERG CORP. L.J. *355 (2007). Mr. Johnson can be reached at (212) 326-0118 or jjohnson@pryorcashman.com.*

** *Steven J. Pierce is a partner in the New York office of Pryor Cashman LLP. His practice area is general corporate and commercial law, with particular concentrations in public and private mergers and acquisitions and commercial transactions. He also has extensive experience in private equity and venture capital financing transactions for established and newly-formed business entities. Mr. Pierce also advises clients on structural, financing and governance issues associated with varied entities, including corporations, joint ventures, partnerships, limited liability companies and similar alternative business entities. The clients for whom he provides services are in varied industries, with a significant number in the technology, computer software, media, entertainment, apparel, publishing and other similar industries. Mr. Pierce can be reached at (212) 326-0139 or spierce@pryorcashman.com.*

*** *David E. Parsly is an associate in the New York office of Pryor Cashman LLP. He represents public and private companies in a variety of general corporate matters, including corporate formation and governance, mergers and acquisitions, corporate finance, and securities issuance and compliance. Mr. Parsly can be reached at (212) 326-0859 or dparsly@pryorcashman.com.*

databases, which consist of two primary components: data and software. Data is simply factual information, and can consist of a single piece of datum such as a social security number, or a series of complex, interrelated data, such as the complete genome of a micro-organism. The software is the tool that enables the database user to manipulate and access the data; it endows a database with useful functions, such as the ability to search the included data, to organize the data in a particular way (e.g., alphabetically), and to modify the data or add new data.

Issues

Database transactions raise questions and issues that, for many lawyers, are unique or rarely encountered. In conducting due diligence, it is crucial to inquire into how the data was obtained, who has the right to access the data, and what types of uses are permissible, including whether third parties given access to the data may disclose it to others. It is typically the case that both the data and software elements of a database consist of some data and software that is proprietary to the seller, and some data and software that is licensed to the seller. Securing licensed rights typically involves consents and, in some cases, negotiations, with third party licensors.

The transfer of the data and software also raise attendant intellectual property questions, such as whether the data is subject to copyright or contains trade secrets, and even, in unusual cases, whether the proprietary software is covered by patents. Moreover, database transactions may run up against regulatory compliance issues if the data, for example, constitutes private health information subject to stringent privacy and nondisclosure mandates of the Health Insurance Portability and Accountability Act (HIPAA).[1]

Finally, in addition to regulatory compliance, lawyers must review the contractual compliance issues involved in the transfer of the database. The data may be subject to certain privacy policies or nondisclosure, subscription, or end-user agreements. As "Database M&A" becomes a more common practice, it is critical for M&A lawyers to consider these issues as they plan for, negotiate and complete database transactions.

Due Diligence

We are all aware that due diligence of the target company's assets plays an essential role in every M&A transaction. In a transaction where a database is perceived to be a significant asset of the target company, however, due diligence must be conducted not only with respect to the data within the database (including the source(s) and permitted uses of the

1. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat 1936 (1996) (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C. and 42 U.S.C.).

data), but also with respect to the software that permits the owner or end-user to access and manipulate that database.

The Software

From the prospective purchaser's perspective, the inability of the target company to convey to the purchaser legal title to the software (if owned) that controls the database, or the right for the purchaser to continue to use that software on the same terms and conditions which the target used it (if licensed), would likely have a material impact on the value of the database to the purchaser.

Proprietary Software

If the software is purported to be owned by the target, issues typical of M&A transactions for the acquisition of software must be considered. For instance, due diligence must be performed to determine whether the target company properly acquired exclusive ownership rights to the software which can be transferred to the purchaser. Counsel for the purchaser will need to review whether the development of the software was performed solely by bona-fide employees of the target company (ideally each of whom will have executed an effective assignment to the target company of all proprietary rights in and to the software), or whether all or any portion of the software was created by third-party independent developers. To the extent third-party developers were engaged by the target company, the purchaser will need to satisfy itself that each third-party developer (including each independent contractor of that third-party developer) has conveyed to the target company all intellectual property rights in and to such software. In addition, as software development is increasingly outsourced to non-U.S. developers, counsel to purchasers may also need to consider the effect foreign laws may have on ownership of the software.

Issues concerning the incorporation of "open-source" or government-funded software should also be considered and may materially impact the value the purchaser ascribes to the software. Government "march-in" rights may limit the buyer's ability to build or expand its customer base. Reliance on "open-source" software may open the window for prospective competitors to more readily develop a database with comparable functionality.

Third Party Software

If the software, or any portion thereof, is licensed from a third party, the purchaser will need to carefully review the relevant license agreement(s) to ensure itself that the licensed software can be conveyed to the purchaser, and that the continued use, or expanded use, of such licensed software by the purchaser is permitted under the terms of such license(s); frequently, consents are required to transfer these licenses.

Because the third-party software is often "off-the-shelf" software that is widely available to commercial users on a non-exclusive basis, it may be impossible to obtain the necessary consents to assign the license. In these cases, the mere fact that a non-exclusive license is readily available to the purchaser may not be sufficient. The database may rely on a "customized" version of the software, in which case the purchaser will need to duplicate those customizations, and ensure that it has access to the resources necessary to maintain and update that software in its customized form.

Source of Data

When analyzing the source of the data comprising the database, purchaser's counsel must also determine whether the data was compiled by the database owner itself, was acquired from one or more third parties in purchase transactions or whether it was licensed from one or more third parties. To the extent that data was compiled by the target company, the purchaser will need to ensure itself that the data was lawfully compiled and/or mined by the target company, in compliance with any applicable regulations and any subscription agreements or "terms and conditions" applicable to the target company's customers or end-users.

To the extent that data was licensed from third parties, the relevant license agreements should be reviewed to ascertain whether that data could be conveyed to the purchaser in the sale transaction, or whether that data is subject to restrictions on use that would prevent its resale to the purchaser, even if the transaction in question is a sale of the stock of the target company or substantially all of the assets of the target (or of a particular division or line of business).

Use of Data

Typically, data is subject to restrictions on use, access and resale, whether by statutes, contract or a combination of both.

Statutory Restrictions

There are several statutes that govern the collection, access, use and distribution of electronic data. For instance, private health information is subject to significant restrictions on its disclosure pursuant to HIPAA, while financial institutions are subject to similar limitations arising pursuant to the Gramm-Leach-Bliley Act (Gramm-Leach-Bliley).[2]

The purchaser may need to satisfy certain criteria to ensure that it is lawfully permitted to review and/or obtain the data from the target company in accordance with HIPAA or Gramm-Leach-Bliley. A discussion of HIPAA, Gramm-Leach-Bliley and other statutes which must be consid-

2. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

ered in the context of database acquisitions is set forth below in the section entitled "Regulatory Compliance."

Contractual Restrictions

Data may also be subject to restrictions on its use and resale by contracts governing the collection and use of such data. Typically, website privacy policies and "terms of use" commit collectors of data to certain restrictions on re-use. Similarly, the terms of any contracts entered into with more traditional suppliers of data, such as media companies and data aggregators, and the terms and conditions to which customers of the target company agree when providing personal information, may contain privacy and/or other restrictions on the use or further disclosure of such data that are binding on the target company.

In addition, if these contracts contain absolute restrictions on disclosure of such data to third parties, then, unless an exception is contained therein for disclosure to a prospective purchaser of the target company or its assets, even the preliminary step of disclosing the data to the prospective purchaser of the database in the due diligence process may be problematic and result in a technical breach of the applicable agreement. From the perspective of counsel to a company which is entering into arrangements to acquire data from third parties, by license or otherwise, it is important for any such license or acquisition agreement to expressly permit disclosure in the context of a potential sale of the business.

The right of the purchaser to access and use the data contained within the database will be determined after consideration of a number of factors. As illustrated above, first it must be determined if the purchaser is permitted, in accordance with applicable law and contractual restrictions, to acquire the data and use it either in the continuation of the existing business of the target company or in a use which is an extension of that business or a "new" business altogether. That is, is the purchaser's intended use of the data also permitted in accordance with applicable statutes and contractual restrictions applicable to the data.

IP Coverage

The sale or other disposition of a database will implicate intellectual property rights. If the data is covered by copyrights, registration of those copyrights may or may not be an issue.[3] The data may alternatively constitute trade secrets. In the United States, trade secrets are a creature of state common and statutory law. A trade secret is generally defined as non-public information that has economic value by virtue of its not being generally known and not being easily determined by others to whom its

3. Broadly speaking, copyright covers any original work of authorship that is fixed in a tangible medium of expression (*see*, 17 U.S.C. § 102 (2006)); however, in the United States, the ability to enforce the copyright in legal proceedings requires that the copyright be registered. 17 U.S.C. § 411(a) (2006).

disclosure would have value, and the further dissemination of which is both limited and protected by the reasonable efforts of those who control it.[4] In rare cases, the software that is used with a database may be protected by patents or, perhaps more likely, may be the subject of one or more pending patent applications. This raises concerns regarding the reliance upon, and likely the scope and enforceability of, those patents.[5]

Copyright

In *Feist Publications, Inc. v. Rural El. Serv. Co.*,[6] the Supreme Court determined that databases themselves are not inherently "original" copyrightable works. Thus, aggregations of data cannot be protected by copyright if the data itself is incapable of alternative means of expression. By way of example, there is only one way to identify a particular person's social security number, whereas there are infinite ways to describe, in words, a person's work experience. As a result, copyright protection for a database consisting solely of individual names, each matched with the individual's social security number, will probably not be available, whereas a database consisting of narrative descriptions of the work experience of those same individuals may well be protectable.

Even if a database is capable of copyright protection, it is necessary to register the copyright in order to enforce it against alleged infringers. In many cases, the value of a database is inextricably tied to the fact that it is a trade secret, or is otherwise not widely available to the public. Registration of the copyright requires, with limited exceptions, public disclosure of the contents of that copyright. As a result, many database businesses limit, or avoid altogether, registration of the copyright in their databases.

In the United States, efforts to pass statutes offering copyright or comparable protection for databases, without requiring the necessary copyright element of originality (i.e., information that is capable of being expressed in multiple ways), have not yet succeeded. In many cases, however, a prospective purchaser anticipates exploiting the database on a world-wide basis. Accordingly, a prospective purchaser's counsel must also consider intellectual property protection in other jurisdictions. In Europe, the 1996 European Union Database Directive[7] introduced a *sui generis* "sweat of the brow" concept to protect the effort put into compil-

4. *See, e.g.*, UNIFORM TRADE SECRETS ACT § 1(4), 14 U.L.A. 402-03 (1985 & Supp. 1990) (defining "trade secret").

5. *See, e.g., In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994). Generally, in order to be patentable, software must cause a computer (i.e., a machine) to do something it cannot otherwise do; the software "creates a new machine" because, as a result of the new programming, "a general purpose computer *in effect* becomes a special purpose computer once it is programmed to perform particular functions from program software" *Id.* at 1566.

6. 499 U.S. 340 (1991).

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

ing databases.[8] The Directive provides a fifteen year copyright type protection for databases so long as the database meets very basic criteria, subject to continuous renewal for each new "subsequent investment" into the contents or format of the database. As with general copyright, it is important to appreciate that this protection does not extend to the trade secret elements of a database.

Trade Secret Rights

To the extent a database that is the subject of an acquisition transaction is not widely disseminated and consists of non-public information access to which requires that the user agree to maintain the database in confidence, that database is a quintessential form of trade secret. This is because the mere fact of payment of consideration to acquire the database establishes that, at least in the purchaser's eye, the database has economic value. Most large M&A transactions for databases have a significant trade secret element.

A database that is protected as a trade secret affords the owner the limited protection of a right to seek monetary damages against those who misappropriate the trade secret and, in many cases, a right to enjoin further unauthorized disclosure of the relevant trade secret. It is critical to appreciate, however, that once publicly disseminated, the ability to regain control of the relevant data may be impossible, particularly in light of the speed with which data can be distributed via the Internet and other means of telecommunications.

In order to rely on trade secret laws to protect that database, the owner will have to take reasonable steps to maintain the confidentiality of the database. Typically, this is accomplished with a subscription agreement, terms and conditions or other binding agreement between the owner and the end-user. These agreements will typically identify, and prohibit further disclosure of, confidential information contained in the database, and prohibit reverse engineering, decompiling or other techniques for discovering the source code for proprietary software included in the database. However, even with customary limitations on further disclosure, the disclosure of trade secrets to a large enough audience may erode the necessary element of secrecy and limit or destroy the enforceability of a claim of trade secret status.[9]

---

8. *Id.* Article 3 of the Directive states that "databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright."

9. The *Restatement*, regarding the importance of secrecy to trade secret status, states:

> [T]he subject matter of a trade secret must be secret. . . . Matters of which are completely disclosed by the goods which one markets cannot be secret. . . . Others may also know of it independently, as, for example, when they have discovered the process or formula by independent invention and are keeping it secret. Nevertheless, a substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information.

In the United States, trade secret protection is, for the most part, derived from a mix of common-law principles and individual state laws.[10] Most states have adopted the Uniform Trade Secrets Act (the UTSA), or a modified version of the UTSA.[11] As a result, a prospective purchaser should not assume that the trade secret status of a database is secure based on general principles or pre-closing due diligence; rather, the buyer should be prepared to devote the time and effort necessary to understand how, if at all, the primary features of trade secret protection in the jurisdiction where the buyer intends to conduct its business differ from the jurisdiction where the business was previously conducted. It may be that differences in state law will require changes in the way the business is conducted after the transaction is closed.

Patent Rights

As indicated above, databases are rarely (if ever) protected by patents. The contents of the database themselves are not patentable subject matter.[12] It is, however, possible to patent software.[13] As a result, purchaser's counsel should be attuned to the possibility (though unlikely) that the software used with a database is covered by one or more patents or is the subject of one or more pending patent applications. If a database's software is covered by one or more issued patents, that protection can be very valuable. It affords the patent holder a period of years (ordinarily, twenty from the date the patent application is first filed) during which it can prevent others from practicing the patented invention without its permission.[14]

Many new businesses like to trumpet pending patent applications as a means of enticing investment. As a quick review of the "Risk Factors" section of any private placement memorandum or any Form S-1 filed with the SEC will reveal, however, the mere existence of a pending patent application, or even a patent, does not necessarily provide useful or robust protection. A purchaser will still need to determine whether any existing patents in fact cover the software that is used with the database and, if so, whether those patents are valid and enforceable. Similarly, if the protection is attributable to pending patent applications, rather than an issued patent, the status of that pending application will need to be evaluated;

RESTATEMENT OF TORTS § 757 (1939).

10. *See* JERRY COHEN & ALAN S. GUTTERMAN, TRADE SECRETS PROTECTION AND EXPLOITATION 69 (Bureau of National Affairs 1998).

11. The UTSA has been adopted in forty-five states. Only Massachusetts, New Jersey, New York, North Carolina and Texas have not adopted the UTSA, or some variation thereof.

12. Patentable subject matter is limited to processes, machines, methods of manufacture and compositions of matters. *See* 35 U.S.C. § 101 (2006). Mere descriptions of those processes, machines, methods and compositions are not covered by the patent.

13. *See In re Alappat*, 33 F.3d 1526.

14. 35 U.S.C. §§ 154 and 283.

the simple filing of an application by no means affords any assurance that a patent will in fact be issued.

Regulatory Compliance

Lawyers in database transactions should be aware of different regulatory compliance issues depending on the database, or more specifically, the types of data comprising the database. This section will discuss a few, but by no means all, of the statutes that may apply in certain situations, including HIPAA, Gramm-Leach Bliley, the Fair Credit and Reporting Act[15] (FRCA) and the Children's Online Privacy Protection Act[16] (COPPA).

HIPAA

As briefly discussed above, HIPAA protects the privacy of consumer health information by establishing privacy and security standards to guard against inappropriate uses and disclosure of such information when it is stored or transmitted electronically. HIPAA regulates how certain "covered entities" handle individually identifiable health information, called "protected health information" (PHI).[17] The health information is considered PHI if it can, or reasonably could, identify an individual. Doctors, pharmacists, hospitals, drug companies, health insurers, and companies that support the healthcare industry commonly store and process PHI using sophisticated databases. These databases can be very valuable to the healthcare industry.

HIPAA thoroughly regulates how PHI is stored and transmitted, and to whom it is disclosed. Generally, HIPAA prohibits the disclosure of PHI to persons or entities that do not qualify as either "covered entities" (i.e., health care providers, health plans and healthcare clearinghouses who transmit PHI electronically) or "business associates" (i.e., providers of administrative services to covered entities) unless that PHI has been "de-identified" (i.e., rendered anonymous).[18] Before PHI can be disclosed to any other persons, it must be "de-identified."[19] The de-identification process can be burdensome, requiring either the specific deletion of eighteen enumerated personal "identifiers" from the PHI, or the encryption of the PHI into a form that cannot be readily re-identified, as established by statistical analysis.[20]

---

15. The Fair Credit and Reporting Act, 15 U.S.C. § 1681 (2006).
16. The Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2006).
17. 45 C.F.R. § 160.103 (2005); 45 C.F.R. § 164.302 (2005).
18. *Id.* § 160.103 (2005)
19. *Id.* § 164.514 (2005)
20. *Id.* § 164.514(b) (2005)

Gramm-Leach-Bliley and the Fair Credit Reporting Act

Gramm-Leach-Bliley allows commercial and investment banks to consolidate, effectively repealing the Glass-Steal Act. Of particular note for this article, Gramm-Leach-Bliley contains a privacy rule to protect consumer information collected by financial institutions.[21] The financial privacy rule mandates that the financial institution maintain a privacy policy protecting the consumer's nonpublic information.[22] Additionally, Gramm-Leach-Bliley requires financial institutions to provide their clients with a privacy notice explaining what information about the client the institution has, when and if the information is shared, and the types of safeguards in place to protect that information.[23]

The Fair Credit and Reporting Act (FCRA) requires that the privacy notice explain to the consumer her right to "opt-out" of the dissemination of her financial information to third parties.[24] The FCRA itself regulates the collection and reporting of consumer credit information, and regulates credit reporting companies. However, the FRCA may apply to compilers of databases who would not describe themselves as credit reporting companies, but who collect similar information and distribute enough information covered by the FRCA to fall within the purview of the statute.

Gramm-Leach-Bliley and the FCRA apply to Database M&A deals in a similar way as HIPAA. As with HIPAA, both parties must be careful to know the contents of the relevant database, make sure that disclosure of the data to the purchaser is authorized under Gramm-Leach-Bliley and the FCRA, and ensure that Purchaser's intended use of the data will also be in compliance with these statutes.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) applies to the online collection of information relating to children under thirteen years of age.[25] COPPA imposes upon website operators a duty to protect the safety and privacy of young children, and identifies when express consent must be obtained from a parent or guardian before that information can be collected or disseminated, and imposes restrictions on the type of marketing that may be directed at young children.[26] Similar to the statutes discussed previously, COPPA raises regulatory compliance issues in database transactions when databases contain information collected from the online activity of children under thirteen.

---

21. 15 U.S.C. §§ 6801-6809 (2006).
22. *Id.* § 6802 (2006).
23. *Id.* § 6803 (2006).
24. *Id.* § 6802(b) (2006).
25. *See id.* §§ 6501-6506 (2006).
26. *Id.* § 6502(b) (2006).

Increasingly, commercially valuable databases include data aggregated from users of websites. When those websites target children under thirteen, or are known to have users who are under thirteen, the use and dissemination of that data is governed by COPPA.[27] Owners of data governed by COPPA must not only protect against unauthorized use and distribution of that data, but must also be prepared to delete or otherwise destroy any such data upon the request of a parent or guardian of the child to whom such data relates.[28] If that data is stored in a database that is utilized as part of the operation and maintenance of a website directed to children under thirteen, the website itself must also include functionality necessary to allow parents of users under thirteen to learn what information about their children is stored in the database, and to revise or delete that data.[29]

Contractual Compliance

Similar to the intellectual property and regulatory compliance issues discussed above, database transactions also raise contractual compliance issues. Many databases are assembled through contracts allowing the database developer to incorporate into the database particular data or aggregations of data. Such contracts include website privacy policies and "terms of use," nondisclosure agreements and traditional contracts pursuant to which data aggregators (e.g., financial institutions) provide data to compilers and distributors of that data (e.g., credit reporting agencies). On the opposite side of the process, when commercializing a database, it is usually subject to some form of distribution, subscription or other agreement between the owner of the database and the end-users of that database. In either case, it is important to avoid making the assumption that, simply because data is included in a database, there are no contractual restrictions on its re-use or disclosure.

Data Sourcing Contracts

Even if the aggregation, use or dissemination of particular data is not subject to regulation, the entity acquiring that data may very well enter into contracts that restrict or otherwise limit how that data is subsequently stored, accessed, re-used or disclosed to others. Sometimes, the data is provided by individual consumers. Perhaps the most well known type of agreement in this category is the website privacy policy. Websites routinely describe for their users how they collect, store and re-use information provided by those users. Sometimes, these policies are separately set forth in the website's "terms of use" section. In either case, if a database includes information provided by users of a website, that web-

27. *Id.*
28. *Id.* § 6502(b)(1)(B) (2006).
29. *Id.*

site's privacy policy or terms-of-use section may well constitute a binding and enforceable contract governing how the relevant data is used.

Similarly, agreements with data aggregators and other parties that engage in the business of collecting data, and providing that data for use in the databases of others, often substantially restrict how that data may be used by the recipient. In many ways, these arrangements amount to database sub-licensing relationships, where a recipient is authorized to incorporate the sourced data into a larger database that is then made available to others. Examples of this type of entities that rely on this type of relationship are credit reporting agencies and large data service providers like *Lexis/Nexis*. In each instance, the critical question is what limitations, if any, are imposed on use and dissemination of the data by the sub-licensee. These are substantively the same concerns that an end-user must consider when it subscribes to a database as discussed below.

Data Dissemination Contracts

Data dissemination contracts are agreements between the entity that owns the database and its customers. For example, when a law firm subscribes to *Westlaw*, there is a detailed agreement pursuant to which the firm and its employees are permitted to access, use and extract information from the database, but the agreement will set forth certain specific restrictions on the use of that information. Typically, those restrictions expressly include a prohibition on redistributing the information or making more than a limited number of copies of the information.

From the purchaser's perspective, a critical concern with these contracts is ensuring that they do not grant to end-users sufficient rights to effectively redistribute the database in competition with the company to be acquired. Ordinarily, confidentiality requirements, limitations on copying and redistribution, and security provisions (e.g., password-protected access) can be sufficient protections, but enforcement of these contractual limitations can be difficult in the context of electronic databases. Accordingly, it is critical to ensure that appropriate limitations, and robust security provisions, are not only contractually required, but also in fact properly and consistently implemented.

CONCLUSION

While Database M&A on the surface is quite similar in practice to any ordinary M&A deal, the complexity of dealing with the issues specific to databases make Database M&A a unique practice. The purpose of this article was to illustrate the issues germane to database transactions, and alert lawyers to the potential pitfalls involved. It is crucial to appreciate the complexity involved in determining the legal status of all the data contained in the database amidst the intellectual property, regulatory, and contractual minefields discussed in this article. When the database is the main focus of the transaction, lawyers should pay closer attention to the issues involved as a matter of course. However, in those deals where a

company's database is just one of many assets obtained, remember that the database contains its own special series of legal issues. As databases continue to grow in value with greater applications, so too will the need to ask and answer the proper questions when engaging in Database M&A.