

Statement of

Keith Kupferschmid
Vice President,
Intellectual Property Policy and Enforcement
Software & Information Industry Association (SIIA)

On Behalf of the
Coalition Against Database Piracy

Before the

Subcommittee on Courts, the Internet and Intellectual Property
of the Committee on Judiciary

and

Subcommittee on Commerce, Trade and Consumer Protection
of the Committee on Energy and Commerce

U.S. House of Representatives

**H.R. _____, THE “DATABASE AND COLLECTIONS OF
INFORMATION MISAPPROPRIATION ACT”**

September 23, 2003
2141 Rayburn House Office Building

Summary

America's database producers have invested hundreds of millions of dollars to collect, organize and maintain information contained in thousands of databases. These large investments have been made to provide easy-to-use valuable information to users in settings ranging from the general public to business and specialized user communities—information that is important in their work and everyday lives. It is critical that database producers be able to protect their investments and encourage new investments in these important information resources.

Misappropriation of databases threatens the availability of organized, timely, comprehensive information. If investments in databases continue to be destroyed, there will be fewer and fewer people willing to make the investment necessary to create and disseminate these valuable database. Moreover, those database compilers who decide to stay in the database business will be forced to keep locked up the information in their databases to avoid destruction of their investment. Inevitably, this will result in fewer and less reliable databases and thus, less information to fuel the information age.

Despite the acknowledged value provided by America's databases, there is presently a lack of meaningful national legal protection for these databases. Certainly, there are some laws available that provide some small amount of protection to database providers, but more often than not these laws fail to adequately deter or prevent databases from piracy. There are a long list of cases that establish this point.

To be clear, we are seeking a very narrowly targeted approach to this problem. We are not seeking "copyright plus," to expand copyright law, to acquire exclusive rights in the database or to lock up information. We are merely trying to protect from free-riders taking our databases and making them available in a way that hurts our businesses. We think this is a reasonable request.

We believe that some of the substantive provisions of the discussion draft, the "Database and Collections of Information Misappropriation Act," will provide protection against database piracy while also accounting for the legitimate concerns of database users through narrowly-crafted exceptions and limitations on liability. Like many other stakeholders, we have concerns with the language used in some of the provisions of the draft. Most significantly, we believe the language in some of the provisions – notably the preemption provisions and time sensitivity provisions, among others -- is somewhat ambiguous and could cause inadvertent consequences. Equally as disconcerting, is that the discussion draft does not recognize database thefts that cause noncompetitive economic harms that adversely affect ISPs and others that have commercial databases. We look forward to working with the Committees to ensure that any preemption of state law is narrowly tailored and does not impede effective licensing of databases or other measures that might otherwise be available, and seeking some appropriate clarifications of the text, including protection against database theft when carried out by or on behalf of parties other than direct competitors.

Statement Text

Chairmen Smith and Stearns, Ranking Members Berman and Schakowsky and members of both Subcommittees, I appreciate the opportunity to testify before you today on the need for legislation that adequately and effectively protects America's databases from piracy. I also welcome the opportunity to comment on your discussion draft, titled the "Database and Collections of Information Misappropriation Act," and would like to especially thank Chairman Sensenbrenner and Chairman Tauzin for their strong leadership on this important issue. We appreciate the commitment of the two committees to work together to produce and enact meaningful database protection legislation.

I am Keith Kupferschmid, Vice President of Intellectual Property Policy and Enforcement for the Software & Information Industry Association. I am here today to testify on behalf of the Coalition Against Database Piracy (CADP). CADP is an ad hoc advocacy group that was formed for the sole purpose of pursuing enactment of a federal law to prevent misappropriation of databases. Its members include large and small database producers who devote substantial resources in compiling, organizing, and distributing database products and providing services that rely on databases. A listing of those companies and organizations that support meaningful database protection is attached.

Database protection is a critical issue to America's database publishers. These companies and organizations have invested hundreds of millions of dollars to collect and organize information contained in thousands of databases. Database publishers not only collect,

compile, and organize the information, they also keep it updated and reliable. These investments are worthy and deserving of protection. Investments in these databases have been made to provide easy-to-use valuable information to users in settings ranging from the general public to business and specialized user communities—information that is important in their work and everyday lives. The value of reliable and comprehensive databases that these companies make available to researchers, businesses, government officials, and citizens is immeasurable. Farmers use databases to get weather and soil information; lawyers, to rely on legal precedent; doctors, to determine safe and effective medical procedures; workers, to search for new jobs; pharmacists, to understand drug interactions; home buyers, to find the right house, and the list goes on.

Given the important role that databases play in our capital markets, law enforcement, and science and research, it is critical that database producers be able to protect their investments from free-riders and pernicious commercial exploitation and that new investments in these important information resources be encouraged. Protection of database investments will stimulate the economy by creating incentives for investments in new databases and accelerating job growth in large and small businesses in our nation's vital U.S. information industry. U.S. database and directory publishers were estimated to generate \$15.4 billion in annual revenue in 1999.¹ Without effective statutory protection, private firms are deterred from investing in

¹ A few examples of the value of today's databases:

“PoisIndex is an index of approximately one million entries on a wide variety of poisonous substances, including drugs, chemicals, commercial and household products, and biologic substances. Substances are reviewed for entry into the database by a group of skilled medical professionals, who also scan the world's medical literature for pertinent data on toxic exposure and management. Approximately 200 actively practicing clinicians from over 20 countries participate in the editorial and selection process. Each substance entry in the database is linked with up to four full-text documents outlining clinical effects, range of toxicity, treatment measures, and other toxicological information. Software engineers are employed to maintain, test, produce and support the database and the software required to store, edit, sort and retrieve the data. The typical PoisIndex user is a medical professional, usually an

database production, resulting in fewer jobs and a shortfall of reliable, accurate and up-to-date information. Protection will promote investments in the creation of new jobs and information services, increase the pace of technological progress, and fulfill the economy's growth potential.

While databases play a key role in supporting America's information based economy, they are also important in protecting our health and well-being. Databases ensure that our prescription medications are safe and will not adversely interact, provide healthcare professionals with vital information on countless topics such as proper antidotes for poisons, and serve as an important resource for mapping out cures for deadly diseases.

Meaningful database protection legislation will also ensure that consumers and businesses have access to the most accurate and reliable information. While database producers are constantly updating their information, those who pirate databases cannot be relied on to do

emergency physician or poison center specialist, who needs instant access to such information in life-threatening circumstances.”

“The MDL Drug Data Report (MDDR), produced by MDL Information Systems ... is a database of approximately 85,000 chemical compounds with potential drug applications. It is updated on a monthly basis from a specialized search of published reports, patent applications and scientific papers so as to make data available on new biologically active compounds as soon as they are disclosed. MDDR tracks these compounds through stages of development and into clinical trials. Accompanying software permits researchers to analyze the effects of modifications of a drug compound's structure on its properties. Researchers can also combine the results of their own internal and external results with the database supplied by MDL to develop their own specialized research tool.”

“Derwent World Patents Index is a comprehensive database of more than seven million separate inventions culled from more than 13 million patent documents worldwide. Coverage includes patents of products from the pharmaceutical industry, agricultural and veterinary medicine, polymers and plastics, chemistry, electronics, electrical and mechanical engineering. All patent information is presented in a uniform, user-friendly format consisting of a simplified English-language abstract explaining key technical details and highlighting applications. In addition to bibliographic information, technical drawings or diagrams are included as available. The Index is updated weekly with information from 40 patent-issuing authorities around the world, 1200 scientific journals, and papers presented at international conferences. Users of the Derwent Index include patent and information professionals, research scientists, engineers, universities, research institutes, libraries, and individual inventors and entrepreneurs.” Examples quoted from a report by Laura D'Andrea Tyson and Edward F. Sherry entitled “Statutory Protection for Databases: Economic and Public Policy Issues.”

the same. As a result, consumers and businesses may end up relying on outdated information, in some cases to the detriment of their health. For example, a mother trying to find the contraindications for a particular medicine could get the incorrect or out-of-date information by unwittingly accessing a stolen outdated database rather than the original compiler's current database.

Consumers need high quality databases which contribute to their ease, productivity, and innovation. Databases save consumers time and effort. Finding that needle in a haystack from diverse and unorganized sources could take an individual weeks or months. Fortunately, database publishers provide quick and easy answers in their databases.

Misappropriation of databases threatens the availability of organized, timely, comprehensive information. If investments in databases continue to be destroyed, there will be fewer and fewer people willing to make the investment necessary to create and disseminate these valuable database. Moreover, those database compilers who decide to stay in the database business will be reluctant to expose their most valuable wares to a thieves' market on the Internet. They will keep tight technical or contractual security on their products and only make them available to smaller, more lucrative markets. Inevitably, this will result in fewer and less reliable databases and thus, less information to fuel the information age.

Despite the acknowledged value provided by America's databases, there is presently a lack of meaningful national legal protection for these databases. While database producers rely on several potential legal theories, none adequately nor effectively deter or prevent database

piracy. Depending on the facts of a particular case, database producers may consider raising claims under: U.S. copyright law, state misappropriation law, state trespass law, state contract law, the Computer Fraud and Abuse Act, federal or state trademark or unfair competition law, and trade secret law. However, none of these claims are sufficient. A list of possible claims and an explanation of their shortcomings is provided in the attached appendix, including references to examples where appropriate. The cases identified here are not an exhaustive list of cases illustrating the shortcomings of the current environment, nor do they capture the scores of instances in which the lack of adequate remedies has prevented database producers from bringing suit to combat known instances of piracy.

In addition to the database piracy cases that have resulted in litigation, there are numerous other instances of piracy that never make it to the court room. Many database producers are unwilling to spend significant amounts of money litigating the questionable causes of action discussed above with the very real possibility that they will lose the case and, in the process, draw attention to the vulnerabilities of the company's databases. For example, National Ad Search (NAS), a Wisconsin-based company, takes and uploads employment classifieds from print newspapers in the top 60 markets and sells them to job seekers. It has no authorization to do so (by contract or otherwise). This type of piracy results in loss of good will of advertisers and customers. Newspapers get complaints from advertisers who place classified ads who continue to get harassed by phone calls long after the ad was published and the job has been filled. Cease and desist letters have failed to deter this company which continues to operate today -- NAS refuses to recognize the newspapers' copyright protection and the newspapers have not found a viable state to bring a misappropriation action. Furthermore, neither the Computer

Fraud and Abuse Act nor section 1201 of the Copyright Act would apply because the initial takings are both non-electronic and unencrypted.

Based on the long list of database piracy cases that have occurred over the course of the past ten years or so there can be no doubt that there is a definite and significant need for database protection legislation. Moreover, the risk of potential future instances of database piracy and the adverse affects such piracy would have on investments in databases and consumer protection is certainly sufficient justification for Congress to enact database protection legislation. Congress has a long history of legislating to protect against potential future harms. In fact, just last session, Congress passed the TEACH Act creating a new exemption in the copyright law in order to encourage certain educational institutions to create distance education courses. There was no demonstrable evidence establishing that an exemption was necessary, but Congress chose to enact the law based on anticipated – rather than actual – problems using copyrighted works for these courses. There is no reason to think that database protection legislation should be treated any differently.

To be clear, we are not seeking “copyright plus,” to expand copyright law, to acquire exclusive rights in the database or to lock up information. We are merely trying to protect against free-riders taking our databases and making them available in a way that hurts our businesses. We think this is a reasonable request. If legislation passes that provides a meaningful legal foundation to fall back on when someone steals a database, companies will be more willing to provide widespread access to their databases and take the risk that it might be stolen. Without this legal basis they are forced to be more cautious about how they disseminate

their databases, how much they should invest in maintaining their databases and, in many instances, whether to create a new database in the first case.

We commend Chairman Sensenbrenner and Chairman Tauzin for their leadership in drafting legislation that seeks to address the problem of theft of our nation's databases. The discussion draft, the "Database and Collections of Information Misappropriation Act" -- reflects years of discussions and negotiations between the Judiciary and Energy & Commerce Committee staff and the stakeholders. The legislation they have developed takes a very targeted and narrow approach to addressing the problem of database piracy.

Unlike prior bills that have addressed the problem of database piracy by providing database producer with exclusive rights to control the use and distribution of a database in any context, the draft legislation developed by the two Committee chairmen, is based on a misappropriation approach that only covers acts of making a database available that cause commercial harm to the database producer. More specifically, the draft legislation creates a narrowly focused prohibition that applies only if ten criteria are met: (1) plaintiff's database must contain a "large number of discrete items;" (2) it must be the result of a "substantial expenditure of financial resources or time;" (3) the defendant must make its database "available in commerce to others;" (4) the amount made available must be at least a "quantitatively substantial part of" the plaintiff's database; (5) the defendant must know that he is not authorized to make the database available; (6) the database is made available "in a time sensitive manner;" (7) the database must serve "as a functional equivalent" of the plaintiff's database; (8) in making the database available the defendant must have caused a loss in revenue to the plaintiff; (9) the

loss in revenue must occur in the *same* market that the plaintiff's database seeks to exploit; and (10) letting this act of misappropriation go unpunished would substantially reduce the incentive of the plaintiff to produce (*i.e.*, create and distribute) the database. These ten criteria – all of which must be satisfied for liability to accrue-- set a very high standard for establishing liability under the draft bill. This standard is even higher when one also considers the exceptions to liability contained in the draft legislation.

We believe that some of the substantive provisions of the draft will provide protection against database piracy while also accounting for the legitimate concerns of database users through narrowly-crafted exceptions and limitations on liability. We also have concerns with the language used in some of the provisions of the draft. Most significantly, we believe the language in some of the provisions – notably the preemption and time sensitivity provisions, among others -- is somewhat ambiguous and could cause inadvertent consequences. Equally as disconcerting, is that the discussion draft does not recognize database thefts that cause noncompetitive harms that adversely affect ISPs and others that have commercial databases. We look forward to working with the Committees to ensure that any preemption of state law is narrowly tailored and does not impede effective licensing of databases or other measures that might otherwise be available, and seeking some appropriate clarifications of the text, including protection against database theft when carried out on behalf of parties other than direct competitors.

We know that a few groups, many of whom were part of the process initiated by the two Committees to come up with a compromise text, have voiced their opposition to the discussion draft. In fact, the discussion draft has a very limited and targeted reach. It protects the database

itself, not the information or facts in a database. The focus of the discussion draft is to protect against unauthorized distributions of a database that cause commercial harm, not to prohibit use or extraction of information from a database. The approach of the discussion draft – relying on a standard of “misappropriation” – is precisely the standard that was recommended by many of those writing now expressing concern.² Their continued opposition amply demonstrates that they simply do not accept the conclusion that the Chairmen have both reached: that Congress should legislate to improve the legal protection available for databases

Just as importantly, several of the letters sent opposing the discussion draft recognize that many of their concerns have been addressed. In particular, the draft will not affect the day-to-day activities of librarians, researchers, scientists, and educators or impede their ability to obtain and use facts. The legal standards to establish liability are extremely high. This is so that only database pirates fall within the draft's reach. The customary activities of a librarian, scientist, or educator would not fall within the reach of this draft legislation. As an additional safety valve, there is an additional exception in the legislation that ensures that nonprofit librarians, scientists, or educators are not swept up by the general prohibition in the discussion draft.

Throughout the process initiated by Chairmen Sensenbrenner and Tauzin we have stated our intention to get narrowly targeted and meaningful legislation that addresses the problem of database piracy while also addressing the legitimate concerns of the database user community.

² In a paper submitted to the two Committees in Spring 2001 groups representing various libraries and universities and industry stakeholders that participated in the database protection discussions and negotiations initiated by the two Committee Chairmen in March 2001 acknowledged that they “would support a true misappropriation bill – for example, one which closely follows the historic standards laid out in *NBA v. Motorola* – which would be constitutional and would not stifle innovation, would not impede scientific progress, and would not ultimately hurt the growth of exciting new database products.”

To the extent that the opponents believe that the draft falls short of this goal, we continue to stand ready to address those concerns in exchange for their support for this important piece of legislation and their recognition that the bill must recognize database thefts that result in noncompetitive harms and address other concerns of the database publishing community on several of the provisions, including preemption of state laws.

We look forward to working with the Congress and the other stakeholders to achieve a legislative solution that eliminates the unfairness we discussed today. Thank you again for all your work on these very complex issues that have arisen before the two Subcommittees and thank you for your commitment and work to address our concerns in this area. I will be happy to answer any questions.

APPENDIX

THE SHORTCOMINGS OF EXISTING LAW

(1) Copyright Law: Copyright law does not provide adequate protection for most databases. Copyright law does not prevent a person from taking the non-copyrightable contents of a database, repackaging or reformatting those contents, and distributing the “new” database. As set forth in the Supreme Court decision of *Feist Publications v. Rural Telephone Service Co.*, 499 U.S. 340 (1991), copyright law only protects a compilation (*i.e.*, a database) if there is sufficient creativity in the selection, arrangement or coordination of the compilation. Most of the characteristics that make a database valuable and user-friendly—its comprehensiveness and its logical order (whether alphabetical in print products or random in electronic products)—are routinely deemed to involve no "creative" selection, arrangement or coordination by the courts.³

³ Prime examples of why copyright law does not protect most databases can be found in:

Warren Publishing, Inc. v. Microdos Data Corp., 115 F.3d 1509 (11th Cir. 1997) *vacating* 67 F.3d 276 (11th Cir. 1995). In this case the Eleventh Circuit reversed the district court's order granting an injunction against defendant Microdos Data for copyright infringement of plaintiff's compilation - a directory of information on U.S. cable television systems. Plaintiff's database contained extensive information on cable systems. The entries were arranged state by state in alphabetical order, and within each state, all of the communities receiving cable television services were also listed alphabetically. Plaintiff collected and arranged all of the information about cable systems by selecting the principal community served by a particular cable operator and then cross-referencing additional communities to the principal community listing. Defendant copied plaintiff's directory into its software package. That software package allowed users to rearrange the data in a format of their choosing and to construct searches of the database.

The Eleventh Circuit found that the plaintiff's selection of cable systems contained in its database did not meet the originality requirement under copyright law because the database included all cable systems and, thus, there was no creativity in the selection of what systems were included in the database. In effect, the plaintiff could not prevail because its database was comprehensive. Since the defendant's software left the arrangement of the system up to the user, even if the court had held the arrangement of the data to be copyrightable (which was unlikely because the data was arranged in alphabetical order), there could not have been a copyright infringement because the defendant did not copy the arrangement.

Mid America Title Co. v. Kirk, 59 F.3d 719 (7th Cir. 1995). Mid America, a company that produces compilations of land title data, sued James Kirk for copyright infringement after it discovered that Kirk had copied

For example, (i) if a database includes all the facts on a given topic, the court will hold that there is no creativity in the selection because every item in that universe was selected; (ii) if a database is arranged in an order that is logical and useful to the user, the court will hold that there is no creativity in the arrangement because the order is typical; and (iii) if an electronic database is in random order and arranged by the user according to parameters established by the user, the court will hold that there is no creativity in the arrangement because there is no arrangement at all. Therefore, the more useful, complete, and up-to-date a database is (*i.e.*, the qualities that benefit database users the most), the less likely it is to be protected by copyright.

Even when courts find that a database contains elements of selection, arrangement or coordination that are creative enough to warrant copyright protection, the scope of protection afforded has been extremely narrow. For instance, the usual standard for determining copyright infringement is whether there is "substantial similarity" between the allegedly infringing work and the copyrighted work. However, where databases are involved, the standard is heightened to a "virtually identical" standard. That standard has led many courts to hold that a copyrighted

one of its compilations. The district court held that neither the selection nor the arrangement of the Mid America database was sufficiently creative to qualify for copyright protection and thus, there was no copyright infringement. The appellate court agreed, expressly acknowledging that the large "amounts of time and effort which Mid America invested in order to gather and report such information [was] irrelevant."

Skinder-Strauss Assocs. v. Massachusetts Continuing Legal Edu., Inc., 914 F. Supp. 665 (D. Mass. 1995). Skinder-Strauss Associates, the publisher of the Massachusetts Lawyer Diary and Manual, known as the "Red Book," sued its competitor MCLE, which publishes the Massachusetts Legal Directory, known as the "Blue Book," for copyright infringement and unfair and deceptive trade practices under Massachusetts law. In creating its directory, the plaintiff listed actively practicing Massachusetts attorneys and judges alphabetically and by jurisdiction. The court found that such arrangement by geography and selection by active bar membership was "typical for any attempt to compile a legal directory for a certain service area." Consequently, the court found that the plaintiff "did not even exercise a minimal degree of creativity...." and that the directory lacked the requisite originality to be protected by copyright. Moreover, the court held that even though "most of the listings published in the Red Book also appear in the Blue Book" (including the fictitious names (*i.e.*, seeds) planted by the plaintiff), the plaintiff's database was not copyrightable; and thus, there could be no copyright violation. In addition, the court held that plaintiff's claims for unfair and deceptive trade practices were preempted by copyright law.

database is not infringed even when the differences between the original database and the copied database are trivial. Courts have also ruled that no infringement occurs when any elements of selection, coordination, or arrangement of the database that was copied did not constitute creative authorship. Accordingly, while some databases may receive copyright protection in theory, in practice the scope of this protection has proven to be minimal.⁴

It has been suggested that Section 1201 of the U.S. Copyright Act would provide a sufficient remedy against database piracy. There is no legal or factual support for this conclusion. Section 1201 was enacted as part of the Digital Millennium Copyright Act (DMCA). It prohibits both the act of circumventing technological protection measures to gain unauthorized access to copyrighted works and the trafficking in any anticircumvention tools that permit unauthorized access. This provision does not come remotely close to addressing the real problem of database piracy because, most significantly, it only applies when the underlying work that is protected by the technological safeguard is a copyrighted work. As noted above, many

⁴ One example of this occurred in *EPM Communications Inc. v. Notara Inc.*, 56 U.S.P.Q.2d 1144 (S.D.N.Y. 2000), where the U.S. District Court for the Southern District of New York found insufficient evidence of similarity to issue a preliminary injunction against a website accused of infringing a printed compilation of licensing sources. EPM Communications Inc. sued Notara Inc. for copyright infringement, alleging that Notara copied substantial portions of its "Licensing Letter Sourcebooks" in Notara's www.notara.net website. Citing the Feist decision, the court found at the outset that EPM's Sourcebooks were entitled to copyright protection as factual compilations because their creation required the selection of businesses of interest to persons involved in licensing. That selection and subsequent arrangement, when viewed in the aggregate, was sufficiently original to be copyrightable.

As to infringement, however, the court denied the plaintiff's request for a preliminary injunction even after acknowledging that Notara copied fifty-five percent (55%) of the listings in EPM's Sourcebook. The court explained that comparison of a printed compilation and an electronic data base was difficult because the arrangement of the printed compilation could not be perceived in the electronic database unless someone uses the computer "to re -arrange the [database] material into the [Sourcebook] copyright holder's arrangement."

Another recent example of this occurred in *Schoolhouse Inc. v. Anderson*, 2002 U.S. App. LEXIS 63 (8th Cir. 2002). Schoolhouse publishes a magazine marketed to prospective home buyers. The magazine features tables of information on area public and private schools. On January 9th, 2002, the U.S. Court of Appeals for the Eighth Circuit held that defendant's copying and posting of approximately 74%-87% of plaintiff's database of school information on its website did not infringe the plaintiff's copyright in the selection and arrangement of its database.

databases are not protected by copyright and, therefore, could not receive the protections afforded by Section 1201. In sum, the same problems that exist with regard to protecting databases under copyright apply to database providers seeking to assert claims under Section 1201. In fact, those difficulties are elevated in a Section 1201 claim because not only does the database producer have to successfully leap the hurdle of proving that the database was protected by copyright, but also must prove that a technical measure was circumvented in violation of the criteria set forth in Section 1201. In addition, section 1201 provides no remedy against a person who distributes a pirated database that was received from a person who circumvented a technical measure to get it.

Furthermore, access control measures protected under the DMCA, like other technology-based solutions, are, at best, only a partial solution. Technical measures do not work at all where the database is in nonelectronic form, such as classified ads in print newspapers, or directories, such as the McGraw-Hill Companies' World Aviation directory. Similarly, it would not apply to Internet companies, such as eBay, Reed-Elsevier and ExpertPages.com, that elect to allow their customers and users to have open access to some or all of their databases. So, while technological protections may be useful in some business models, in many others they are not.

(2) State Misappropriation Law: State misappropriation law does not provide meaningful national protection to databases. First, each state's misappropriation law -- which is usually a common law doctrine -- is different. In the Internet environment this proves problematic. For example, when a company makes its database available over the Internet,

The court found that, although the defendant admitted to copying the database, much of what was copied was attributable to an inevitable selection and obvious arrangement of topics that lacked copyrightable originality.

should it prevent persons from states without misappropriation laws or with inadequate misappropriation laws from accessing its database? Even if it wanted to prevent such access, how would it do so? National uniformity is clearly needed in this area.

Second, many state misappropriation laws are restricted to “hot news”. Under these regimes, a database might be protected if it contains "hot news," but only for a short period of time, such as the first fifteen minutes after its inception. The great majority of databases, however, have a value long after the fifteen minutes have expired.

Third, because state misappropriation laws are largely common law, many courts have held their respective state's misappropriation laws to be preempted by federal copyright law.⁵ Thus, there must be federal legislation that addresses the misappropriation of databases.

(3) State Trespass Law: State trespass law provides a remedy against database piracy only in the rarest of cases.⁶ A significant limitation on state trespass claims is that they do not

⁵ Another example of database piracy for which a misappropriation claim (and several other state claims) proved unavailing occurred in *Information Handling Services, Inc. v. LRP Publications*, 54 U.S.P.Q.2d 1571 (E.D. Pa. April 18, 2000), 2000 Copr. L. Dec. P28,177 (E.D. Pa. Sept. 20, 2000). Information Handling Services (IHS), a company that creates value-added databases of publicly available government information, brought the action when it found that LRP had copied its product and produced a less expensive alternative. Consequently, IHS "suffered significant losses." As a result, IHS sued on several theories, including violations of state unfair competition laws, misappropriation laws, and trade secret laws. However, the District Court for the Eastern District of Pennsylvania held that each of these state law claims, except for the contract claims, were preempted by the Copyright Act. In addition, the court expressed doubt that the contract was enforceable, but because the court was merely deciding a motion to dismiss, it determined that the ultimate enforceability of the contract did not need to be decided. See also *Ticketmaster v. Tickets.com*, discussed below, and *Lowry's Reports, Inc. v. Legg Mason, Inc.* 186 F. Supp. 2d 592 (D. Md. 2002), in which Legg Mason employees posted a single subscription email report to a company intranet and distributed the report internally, a federal court in Maryland held that Lowry's hot news misappropriation claim was preempted by copyright law. The court stated that "[f]ree-riding' . . . , the only element that constitutes a wrongful act, seems indistinguishable from the right to reproduce, perform, distribute or display a work. The other elements do not describe any behavior at all. The cost of generating the information, its time sensitivity, and direct competition between the parties merely define pre-existing conditions; the threat to the plaintiff's business merely 'identifies a consequence of the act of 'free-riding'."

apply to non-electronic databases or databases distributed on CD-ROM. Also, trespass claims will likely only be successful where a plaintiff can prove server or network damage. Most database publishers are not likely to be able to prove this.⁷

In addition, because of the novelty of applying state trespass claims to the Internet, there is no guarantee that other states will interpret these claims the same way that the district courts in California and New York did. As in other cases of reliance on state law, there are substantial variations among states, and national uniformity is needed. Once again, this highlights the need for a uniform federal law providing meaningful database protection.

⁶ See *EBay v. Bidder's Edge*, 100 F. Supp. 2d 1058 (N.D. Ca. 2000). Unlike real-time aggregators, which merely search the relevant web site pursuant to a search request, Bidder's Edge (BE) copied eBay's entire databases by employing automated data extraction tools, called "web crawlers," "robots," or "spiders" to extract eBay auction listings for posting on BE's site. eBay brought several claims against BE, including a trespass claim under California law. The court agreed with eBay's trespass claim, holding that, if BE's crawling activities were allowed to continue unchecked, it would encourage other auction aggregators to engage in similar searching activities. The cumulative effect caused by similar auction aggregators could be severe, possibly causing eBay's system to suffer gaps in service crash altogether (despite the fact that BE's present activities were found to have a minimally detrimental effect on eBay's site). As evidenced in other court cases since this decision, the eBay decision has no applicability to most of the databases on the market. It applies only to those companies that find their services "crawled" by electronic agents to such a magnitude that the hosting system or network may become overburdened. It also important to note that the injunction issued in this case: (1) does not prevent the pirate from distributing the information it extracted, (2) does not apply outside the state of California, and (3) does not protect database publishers who distribute their databases on printed materials, CD-ROMs, or other traditional media. See also, *Register.com v. Verio*, 126 F.Supp.2d 238 (S.D.N.Y. 2000), on appeal.

⁷ The limitations on a trespass claim can be seen in the case of *Ticketmaster v. Tickets.com*, 2000 WL 1887522 (C.D. Cal. August 10, 2000); 2001 WL 51509 (9th Cir. Jan 8, 2001); 2003 Cop. L. Dec. P. 28,607 (C.D. Cal. March 7, 2003). The facts are as follows: Tickets.com established a deep link to the concert information located on Ticketmaster's web site. When Ticketmaster became aware of the deep link, Ticketmaster sued Tickets.com under various claims based on the unauthorized deep linking. After the court ruled against Ticketmaster, Ticketmaster implemented technology which prevented deep-linking to its concert listings. Tickets.com thereafter found a way to circumvent this technology by using "spiders" or web crawlers to copy Ticketmaster's internal web pages, extract the concert information (such as the date, price, time, venue, and band playing) and post it on Tickets.com's web site in a different format. Ticketmaster then sued Tickets.com for copyright infringement, breach of contract, misappropriation and trespass. None of these claims were successful and no injunction was issued. With regard to the trespass claim, the court found that the facts presented by Ticketmaster were compellingly different from those offered by eBay in its lawsuit against Bidder's Edge. Unlike the situation in the Bidder's Edge case, Ticketmaster could not "present the spectacle [sic] of dozens or more parasites joining the fray." Ticketmaster subsequently lost its

(4) State Contract Law: Contracts are only effective against the people who assent to them. Sometimes the database pirate is a customer. But more often the pirate is an unrelated third party. If a database producer has no contractual relationship with the database pirate, there is no way for the database producer to bring a case against the database pirate for breach of contract under state law. The other problem with state contract law is that because it differs from state to state, database providers and users may find themselves faced with different results in different jurisdictions.⁸

(5) Computer Fraud and Abuse Act, 18 U.S.C. 1030: The Computer fraud and Abuse Act is an anti-hacking statute that offers little protection against database piracy. It does not apply to printed compilations, or to compilations stored on CD-ROM or other similar media. Thus, while Section 1030 may work for some business models, for many others it does not. Finally, similar to the state trespass claims discussed above, section 1030 would only apply where a system or network itself is harmed. It would not apply where the market for or value of the database is harmed as opposed to the network or system on which the database resides being harmed.

appeal. Remarkably, the *Ticketmaster* case was decided by the same court that earlier had held for eBay on its trespass claim.

⁸ The problems with state contract law are evident in several cases. *Capital Asset Research Corp. v. Finnegan*, 160 F.3d 683 (11th Cir. 1998), involved Capital Asset Research Corp (CARC), a company that is in the business of purchasing tax executions (or liens) and tax deeds on real properties for which property taxes are owed. CARC created a database of property-specific information, tax redemption behavior, and final bid guidelines for tax deeds sold at auction. A former employee of CARC copied the databases and gave the copied databases to CARC's competitor, who used the databases to compete against CARC in purchasing properties. CARC sued for breach of contract and violations of trade secret and it lost on all claims. The court found that the database did not meet the necessary criteria to qualify as a trade secret because among other things the information contained in the database was publicly available. The court also found that there was no breach of the non-compete clause in the contract and thus, no breach of contract. See also *Ticketmaster v. Tickets.com*, discussed above. In addition, groups like the National Association of Realtors recognize that, although there may be remedies against authorized users (MLS participants) based on contracts or licenses, those remedies do not apply to "third party" pirates who steal the data off the Internet.

(6) Federal or State Trademark or Unfair Competition Law: Existing trademark and unfair competition laws are insufficient because they require that a database producer prove a likelihood of confusion. If there is no confusion, there is no cause of action.

(7) Trade Secret Law: Few databases can be protected by trade secret. In virtually all cases the contents of the database are available to the public and therefore are not protected by trade secret law. Assuming trade secret law does provide a measure of protection for non-public databases, relying on it to protect databases in general creates incentive for database producers to privatize their databases in order to protect them as trade secrets. That incentive is contrary to the notion that databases should be shared with the public.⁹

⁹ See *CARC v. Finnegan*, discussed above.