JENNER&BLOCK Intellectual Property and Technology Law Practice

Intellectual Property News SPRING 2003

New Data Security Law Has Widespread Effect

by Adam Petravicius and Sarah Walkington

Adam Petravicius is a partner in Jenner & Block's Chicago office and a member of the Firm's Intellectual Property and Technology Law Practice. His practice focuses on transactions involving intellectual property and technology, and he regularly counsels clients on Internet and e-commerce issues. He received his bachelor's degree in Electrical Engineering from the University of Michigan, magna cum laude *and graduated* magna cum laude *from Harvard Law School.*

Highlights

Sparked by concerns about privacy and identity theft, California recently enacted a sweeping law that will require companies to disclose computer security breaches involving—or reasonably believed to involve—the personal information of a California resident. This new law will likely affect any company with customers or employees in California, as well as service providers that maintain data on behalf of any such company. Moreover, this law may become a national standard as other states and even the federal government enact similar laws.

California Senate Bill 1386

In April 2002, hackers broke into the payroll database for the State of California and obtained personal information on about 265,000 state employees, including their names, home addresses, social security numbers and bank account information. The state agency that ran the database failed to discover the security breach for more than a month and, worse, failed to notify the affected employees for more than two weeks after discovering the breach.

Prompted by this incident and the increasing risk to individuals' privacy and financial security due to the widespread collection of personal information in both the private and public sector, California enacted a new law. California Senate Bill 1386 ("SB 1386") requires California residents to be notified of computer security breaches involving their personal information. SB 1386 will become ***effective on July 1, 2003***.

Companies That Must Comply

SB 1386 applies not only to state agencies but also to any company[1] that conducts business in California and ***owns or licenses*** computerized data that includes ***personal information*** about a ***California resident***. Although not clear from the statute, given the incident that prompted its enactment, a company with California employees likely qualifies as a company conducting business in California with respect to those employees. SB 1386 also appears to apply to service providers who maintain such data on behalf of a third party, regardless of whether the service provider otherwise conducts business in California.

Companies that fail to comply with SB 1386 may face civil actions for damages or injunctive relief, which may take the form of class action suits. The provision in SB 1386 providing for civil actions for damages is limited to "any customer" that is injured by a violation and, notably, may preclude employees from seeking damages. However, it is unclear whether the California legislature intended to prevent employees from seeking damages and courts may still enable them to do so. This is especially true given the incident prompting the enactment of SB 1386 and California's general public policy of protecting employees. Moreover, SB 1386 expressly preserves any other rights or remedies available under law, which may provide a separate basis for employees to seek damages. SB 1386 does not limit injunctive relief to any particular class of persons or entities.

continued on page 2

New Data Security Law Has Widespread Effect

continued from page 1

Sarah M. Walkington is an associate in Jenner & Block's Chicago office and a member of the Firm's Intellectual Property and Technology Law Practice. Her practice includes patent and trademark litigation and counseling. She obtained her J.D. from the John Marshall Law School, magna cum laude *where she was a Dean's Scholar, Herzog Scholar, member of the Law Review, and editor and co-founder of the* John Marshall Review of Intellectual Property Law.

When Notice Must Be Given

A company must provide notice of any security breach where the unencrypted personal information of a California resident was, or is reasonably believed to have been, acquired by an unauthorized person. A security breach is defined in SB 1386 as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the [company]." Personal information means an individual's first name or initial and last name ***in combination with*** one or more of the following: (1) social security number; (2) driver's license number or California Identification Card number; or (3) account number, credit card number or debit card number along with any required security code, access code or password. Personal information does not include information that is lawfully available to the general public from federal, state or local government records.

Notice Requirements

Companies must provide notice of security breaches in the most expedient time possible and without unreasonable delay. Notice must be provided to ***every resident*** whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notice may be provided in writing or electronically (provided it meets the requirements of 15 U.S.C. § 7001 regarding electronic records and signatures). Alternatively, if the cost of providing notice would exceed $250,000, the number of people to be notified would exceed 500,000 or the company lacks sufficient contact information, then substitute notice may be given. Substitute notice must consist of all of the following: (1) an e-mail notice if an e-mail address is available; (2) conspicuous posting of the notice on the company's website if it has one; and (3) notification of major statewide media.

SB 1386 also provides that companies that maintain computerized personal information that they do not own must immediately notify the owner or licensee of such personal information of any security breaches. This provision appears to be directed to service providers that maintain databases for a third party. Notably, this provision is not limited to companies that conduct business in California. In addition, a service provider may technically be considered a licensee of personal information and may be subject to the general notice requirements described above. However, the context of this provision suggests that the term "license" may be limited to beneficial users of personal information and not apply to service providers that simply maintain personal information.

Finally, SB 1386 allows for notice to be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. However, the notice must still be given once the law enforcement agency determines that it will not compromise the investigation.

Controversy Regarding SB 1386

Supporters of SB 1386 assert that mandatory disclosure of security breaches will push companies to take privacy more seriously and to pay more attention to security issues and preventative measures. They argue that notice will allow individuals to take steps to protect themselves from identity theft or other risks resulting from a security breach. Ultimately, they believe, this will result in a higher level of trust and confidence in the use of computerized personal information because no news will mean good news instead of uncertainty about the security of personal information.

Critics argue that the new law may produce the opposite of its intended effect by causing companies to become more lax about monitoring security breaches in order to adopt a "don't ask, don't tell" approach of minimizing their knowledge of security breaches in order to minimize the notices they must give. They believe that companies will fear giving notice of security breaches because it

continued on page 3

New Data Security Law Has Widespread Effect

continued from page 2

could harm their reputation or expose them to litigation. Disclosure could also encourage hackers by giving them bragging rights to a publicized breach or exposing a company's vulnerability. Critics argue that the difficulty in determining whether a particular security breach affected personal information could result in a barrage of notices that misleads people to believe that their personal information is constantly under attack.

Companies may wish to require their service providers to encrypt all personal information...

Effect of SB 1386 Outside California

Although SB 1386 is directed to California residents, it affects every company that has customers or employees in California. In addition, because of California's size and prominent role in the high-tech industry, the new law could create a *de facto* national disclosure policy. Moreover, it is likely to lead to similar legislation in other states. The federal government may also follow suit. U.S. Senator Diane Feinstein has already introduced a draft of a bill, known as the Database Security Breach Notification Act, which would make mandatory disclosure the federal standard.

Compliance with SB 1386

Due to its widespread effect, companies nationwide will need to be prepared to comply with the notice requirements of SB 1386. By taking the following steps, companies may be able to minimize the burden of compliance:

- **Encrypt personal information** – SB 1386 applies only to security breaches involving ***unencrypted*** personal information. As a result, encrypting computerized personal information may be a relatively easy way to avoid having to provide notice. Because SB 1386 does not specify any minimum encryption standard, companies should follow relevant industry standards.

- **Consider involving law enforcement** – By involving law enforcement, a company may be able to delay providing notice of a security breach. Delaying notice may allow the company to later present the security breach in a more favorable light, *e.g.*, by being able to report that the company has cooperated with law enforcement regarding the breach, that the company's security has been improved to prevent the breach from recurring or that the responsible individuals were apprehended by law enforcement.

- **Address this issue with service providers** – Companies that outsource their database management functions should consider how to address SB 1386 and future similar laws in their outsourcing contracts. Companies may wish to require their service providers to encrypt all personal information for the reasons described above. In addition, both service providers and their customers may wish to specify in the contract which entity owns the personal information so that it is clear which entity has responsibility for the general notice requirement under SB 1386.

---

[1] SB 1386 refers to any "person or business." For convenience, this article will use the term "company" to refer to a person or business as contemplated by SB 1386.

Use of a Trademark Is Not "Fair" If Public is Confused

by Lisa Parker Gates

Executives often wonder why some uses of trademarks are considered "fair" while others are not. The United States Court of Appeals for the Ninth Circuit recently had a chance to shed some light on when use is fair and when it is not. The case before the court, *Brother Records, Inc. v. Jardine*, involved the surviving former members of the Beach Boys, the popular 1960s California surf band. When the group was in its heyday, the members formed a company, Brother Records, Inc. The company owned all of the band's intellectual property, including the valuable "Beach Boys" trademark. Several years ago, the company granted Mike Love, one of the band's former members, a license allowing him to tour with his own band under the name "Beach Boys."

Just as Love's tour began, another former member of the band, Alan Jardine, began his own tour under variations of the name "The Beach Boys Family and Friends." Brother Records objected to Jardine's touring under that name, and it refused to grant him a license to use the Beach Boys name. Jardine nonetheless continued to tour using the name. Brother Records claimed during the subsequent trial that club owners were confused about who they were booking for shows, and that fans were confused about which band members they were going to see.

Defending himself against the trademark infringement claim brought against him by his former band mates, Jardine claimed that his use of the Beach Boys name was fair use under the federal Trademark (Lanham) Act. After all, he argued, he used the "Beach Boys" trademark only to describe himself as a former Beach Boy.

The judge found Jardine's arguments unconvincing, siding with Brother Records.

Unauthorized use of a trademark is always fair when it is used only for reference or to describe the owner's products or services. In other words, no one needs permission to refer to the Los Angeles Lakers or a Volkswagen or the World Series or even the Beach Boys (all federally registered trademarks) when the purpose is simply to discuss facts about the things or people those marks represent. As long as the trademarks are not being used to sell goods or services, there is no infringement.

On the other hand, use of another's trademark to describe one's own goods and services is considered fair in certain circumstances. For instance, it is considered fair to use another's trademark to compare goods or services in an advertisement. It is fair for a mechanic's business to advertise that it repairs a certain brand of car. It is fair for a grocery store to advertise a sale of certain brands of paper towels or soft drink.

Similarly, it would most likely be considered fair use if Alan Jardine were to tour as "Alan Jardine, former member of the Beach Boys."

Courts decide whether use of a trademark to describe one's own goods or services is fair by considering whether three requirements are met. First, the product described must be one that cannot easily be described without using the trademark of another. Second, the user may use only as much of the trademark as is necessary to identify the product or service. Third, the user must do nothing that would suggest affiliation with or endorsement by the trademark owner.

The court ultimately sided with Brother Records because it found that Jardine's use of "Beach Boys" during his tour suggested to the public that he in fact was the Beach Boys, not simply a former member of the Beach Boys. On the grounds that the public was confused as a result of Jardine's unauthorized use of "Beach Boys," the court found that Jardine had infringed upon the trademark rights of Brother Records.

The full text of the court's opinion in *Brother Records, Inc. v. Jardine* can be found at http://pub.bna.com/ptcj/0157095.pdf.

U.S. Supreme Court Finds that Victor Did Not Dilute Victoria

by Lisa Parker Gates

The idea that the owner of a famous trademark could stop another from using a trademark that lessened the capacity of the famous mark to identify goods was made black letter law in 1995 under the Federal Trademark Dilution Act. How and when marks actually are diluted has proved a murky area of the law, but a recent opinion of the U.S. Supreme Court provides some guidance for lawyers and trademark owners.

The Dilution Act provides that the owner of a "famous" mark may stop another's commercial use of a mark if that use dilutes the distinctive quality of the mark. In *Moseley v. V Secret Catalogue, Inc.*, the Court reversed and remanded a lower court decision that the famous VICTORIA'S SECRET trademark had been diluted by the defendant's use of VICTOR'S LITTLE SECRET for an adult novelties business.

Victor and Cathy Moseley use the name and mark VICTOR'S LITTLE SECRET for their Kentucky store, where they sell lingerie, adult videos and novelties. The store is located 60 miles from a Victoria's Secret store in Louisville. V Secret Catalogue, Inc., the parent company of Victoria's Secret, sued the Moseleys for federal and state trademark infringement, unfair competition and trademark dilution. A district judge dismissed the infringement and unfair competition claims, finding that there was no likelihood of confusion between the two marks. However, the court granted summary judgment for V Secret Catalogue on the grounds that the use of the VICTOR'S LITTLE SECRET mark was "likely to blur and erode the distinctiveness" and "tarnish the reputation" of the VICTORIA'S SECRET mark. The Court of Appeals for the Sixth Circuit affirmed the district court's decision.

The U.S. Supreme Court found that simply finding that consumers mentally associate the junior user's mark (in this case, the VICTOR'S LITTLE SECRET mark) with a famous mark like VICTORIA'S SECRET is not enough to find dilution under the federal Act. According to the court's opinion, mere mental association will not necessarily reduce the capacity of a famous mark to identify its owner's goods.

The Court emphasized that "blurring" and "tarnishing" are not necessary consequences of mere mental association. Thus, even though a man testified during the trial that he made a mental association between the two stores when he saw an advertisement for the Victor's Little Secret store, he did not necessarily or consequently form any different impression of the store because of the association. He was offended by the advertisement, but that offense did not change his impression of Victoria's Secret.

The case has been remanded to the district court to be heard again under the Supreme Court's opinion.

The court's full opinion in *Moseley v. V Secret Catalogue, Inc.* can be found at http://www.supremecourtus.gov/opinions/02pdf/01-1015.pdf.

Lisa Parker Gates is an associate in Jenner & Block's Chicago office and a member of the Firm's Intellectual Property and Technology Law, and Health Care Practices. She concentrates on intellectual property and technology licensing, trademark prosecution, copyright protection, e-commerce and online law, and non-profit law. She received her masters degree in journalism from the Medill School of Journalism and graduated cum laude *from Loyola University Chicago School of Law, where she served as editor-in-chief and features editor of the Loyola University Chicago School of Law* Public Interest Law Reporter.

Coming to a State Court Near You!

Could Patent Infringement Matters Really End Up in State Court?

by Steven McMahon Zeller

Steven McMahon Zeller is an associate in Jenner & Block's Chicago office and is member of the Firm's Intellectual Property and Technology Law Practice. He focuses on patent and technology litigation, patent prosecution, licensing and intellectual property counseling. Mr. Zeller received his bachelor's degree in mechanical engineering from Iowa State University in 1989 and his J.D. from the Northwestern University School of Law in 1996. While at Northwestern, Mr. Zeller served as a note and comment editor on the Northwestern University Law Review.

Ever since the creation of the United States Court of Appeals for the Federal Circuit more than 20 years ago, it has been taken for granted that an appeal in any patent litigation case could only be taken to that court. In the recent decision in *The Holmes Group, Inc. v. Vornado Air Circulation Systems, Inc.*, 535 U.S. 826 (2002) the U.S. Supreme Court effectively took the Federal Circuit's jurisdiction away in cases in which the original complaint in the district court does not allege a claim arising under United States patent laws.

The most immediate effect of this decision is that the regional circuit courts of appeals will now have jurisdiction over appeals from cases where the patent claims were raised in pleadings other than the complaint, such as a counterclaim. While the pros and cons of this result will continue to be debated, the possibility of a different, and potentially more dramatic, effect of this decision is taking shape. There is a real possibility that state courts could end up deciding patent law claims, particularly those raised in counterclaims.

How could litigation concerning patents, long a subject for federal district courts only, end up in state courts?

It has to do with the analysis employed by the U.S. Supreme Court in the *Holmes* decision. The question presented to the Court was whether the Federal Circuit had appellate jurisdiction over a case in which the counterclaim, but not the original complaint, alleged a claim arising under the federal patent laws. By statute, appeals from cases in the district courts are to be taken to the Federal Circuit only when all or part of the action arose under the federal patent laws. The Court, following precedent on when a case should be in the federal courts, determined that the statute required one or more claims in the original complaint to arise under the patent laws for the district court to have jurisdiction, and thus for the Federal Circuit to have jurisdiction over an appeal. Thus, a counterclaim arising under the patent laws did not give jurisdiction to the federal courts and, as a result, the Federal Circuit would not hear an appeal over such a case.

> *There is a real possibility that state courts could end up deciding patent law claims...*

Prior to the decision in *Holmes*, the U.S. Supreme Court had never explicitly stated that a counterclaim could not serve as the basis for a district court's jurisdiction for patent matters. In fact, the Federal Circuit itself found that a counterclaim arising under the patent laws did give the district courts jurisdiction, and thus provided a jurisdictional basis for the Federal Circuit to hear an appeal from such a case. Now, however, the Supreme Court has made it clear that the original complaint had to contain claims arising under the patent laws for the federal courts to have jurisdiction of the case.

So what does any of this have to do with patent cases in state courts?

The statute that provides jurisdiction to the federal district courts for cases arising under the patent laws also dictates

that the district courts will have jurisdiction of those cases exclusive of the courts of the states. Now, if a district court does not have jurisdiction over a counterclaim arising under the patent laws, it can be argued that the district court does not have jurisdiction exclusive of the state courts. Thus, in theory, a state court can accept a counterclaim asserting patent matters.

Prior to the *Holmes* decision, state courts looked to this same provision to decline to accept jurisdiction over a counterclaim asserting claims under the patent laws. For example, in *American Home Products Corporation v. Norden Laboratories*, a Delaware court found that a proposed counterclaim was equivalent to an original complaint filed by a litigant and that since the court would not have jurisdiction if the claim had been brought in a complaint, the Delaware court did not have jurisdiction over the same claim asserted as a counterclaim. The *Holmes* decision now no longer allows the equating of a counterclaim and an original complaint, making this argument moot.

Recently, the Indiana Supreme Court has recognized the new distinction created by *Holmes*. In *Green v. Hendrickson Publishers, Inc.*, the court recognized that the only basis for finding that the federal courts have exclusive jurisdiction of a claim arising under the copyright or patent laws was found within the jurisdiction statute construed by the U.S. Supreme Court in *Holmes*. Relying on the U.S. Supreme Court's analysis, the Indiana court ruled that a copyright claim is not subject to the exclusive jurisdiction of the federal courts. Thus, a breach of copyright claim presented in the counterclaim, once thought to be the exclusive purview of the federal courts, will now be heard by the state trial court in Indiana.

... a breach of copyright claim presented in the counterclaim, once thought to be the exclusive purview of the federal courts, will now be heard by the state trial court in Indiana.

There is nothing to stop the analysis applied in the *Green* case from being applied to a patent law counterclaim filed in state court. In states that have compulsory counterclaims, it is very likely that state courts will be deciding patent law issues in the near future. Proposals to prevent that result are being discussed in the bar associations and elsewhere, but at this point, no legislation has been introduced in Congress. Potential litigants must now consider the possibility of having a state court judge or jury decide patent law disputes before initiating any litigation that may affect the patent rights of any party.

JENNER&BLOCK

Intellectual Property and Technology Law Practice

Intellectual Property News

SPRING 2003

IP Counsel Notes

Reginald J. Hill will serve as a panel member for a discussion on Patent Prosecution Procedures and Pitfalls entitled "Where Are Your Priorities? 102(e) Changes and Challenges" at the Annual Meeting of the American Intellectual Property Law Association in Washington, D.C. on October 31, 2003. Mr. Hill was also recognized in the June 2003 issue of *Diversity & The Bar* magazine as one of the top attorneys of color for Intellectual Property Law.

Michael S. Walsh lectured on intellectual property and contracts at Northwestern University's Kellogg School of Management on May 21, 2003.

Intellectual Property and Technology Law Practice

The Intellectual Property and Technology Law Practice provides a full range of services including intellectual property litigation; counseling on patent, trademark, domain name, copyright, trade secret, unfair competition, computer and e-commerce law matters; licensing and other corporate intellectual property transactions; and the procurement of patents and trademark registrations.

The practice includes attorneys who hold degrees in electrical engineering, mechanical engineering, physics, computer science, chemistry, biology/ biochemistry, veterinary medicine and other technical fields, many of whom have been admitted to practice before the United States Patent and Trademark Office. Several attorneys had industry experience in their technical fields before their careers in the law, which better enables our attorneys to effectively and efficiently analyze the technical aspects of intellectual property and technology-related matters for the Firm's clients.

Newsletter Contacts:

Stanley A. Schlitter, Co-Chair
312 923-2712
sschlitter@jenner.com

Richard J. Gray, Co-Chair
312 923-2939
rgray@jenner.com

Eric H. Weimers, Editor
312 923-2986
eweimers@jenner.com