FENWICK & WEST LLP

# Intellectual Property Bulletin

Fenwick & West LLP — Summer 2001

FENWICK & WEST LLP

## About The Firm

Fenwick & West LLP provides comprehensive legal services to high technology and life sciences clients of national and international prominence. We have over 280 attorneys and a network of correspondent firms in many major cities throughout the world. We have offices in Mountain View and San Francisco, California and Washington, D.C.

Fenwick is committed to providing excellent, cost-effective and practical legal services and solutions that focus on global high technology industries and issues. We believe that technology will continue to drive our national and global economies, and look forward to partnering with our clients to create the products and services that will help build great companies. We differentiate ourselves by having greater depth in our understanding of our clients' technologies, industry environment and business needs than is typically expected of lawyers.

Fenwick is a full service law firm with "best of breed" practice groups covering:

- Corporate (emerging growth, financings, securities, mergers and acquisitions)
- Intellectual Property (patent, copyright, licensing, trademark)
- Government Contracts and Technology Transfer
- Litigation (commercial and IP litigation)
- Tax

## Our Offices


Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel: 650.988.8500
Fax: 650.938.5200

Suite 200
815 Connecticut Avenue NW
Washington, DC 20006
Tel: 202.261.0400
Fax: 202.463.6520

Embarcadero Center West
275 Battery Street
San Francisco, CA 94111
Tel: 415.875.2300
Fax: 415.281.1350


For more information about Fenwick & West LLP, please visit our Website at: www.fenwick.com.

FENWICK & WEST LLP

# Intellectual Property Bulletin

**Summer 2001**

## Table of Contents

# Section 2019(d)'s "Reasonable Particularity" Requirement Can Leave Litigants Guessing

Tyler Newby (tnewby@fenwick.com)

Anyone who has litigated a trade secret misappropriation case in California in the last decade and a half is intimately familiar, perhaps painfully so, with an aspect of California's enactment of the Uniform Trade Secrets Act ("UTSA") that is unique to this state —Section 2019(d). Cal. Civ. Code § 2019(d) (West 2000). Section 2019(d) bars a plaintiff alleging trade secret misappropriation under Cal. Civ. Code § 3426 *et seq*. from taking discovery until the plaintiff identifies its alleged trade secrets with "reasonable particularity." However, the statute offers no guidance as to the meaning of the seemingly innocuous phrase, "reasonable particularity."

Although anecdotal evidence indicates that § 2019(d) is litigated frequently, both in Superior Court and in federal courts applying California's version of the UTSA through diversity or supplemental jurisdiction, not a single published California state court opinion has addressed the meaning of § 2019(d)'s "reasonable particularity" requirement. The handful of federal opinions that have addressed the statute offer guidance as to the purpose of the statute, but do not address the level of detail with which plaintiffs must identify their alleged trade secrets before taking discovery. This absence of case law and any clear standards is a source of headaches for the courts and litigants—both plaintiffs and defendants—particularly where the alleged trade secrets concern complex technology.

Not surprisingly, defendants and plaintiffs in trade secret disputes rarely agree on the meaning of "reasonable particularity." Plaintiffs typically take the position that they need only identify the broad categories within which the trade secrets are located, such as the manufacturing process for a particular widget, or a customer list for a particular service. Defendants, on the other hand, typically argue that plaintiffs must identify the precise trade secrets, within the meaning of § 3426.1, that plaintiffs allege defendants misappropriated. The absence of reported case law directly addressing this issue puts the unenviable burden on trial courts and discovery magistrates to determine who is right, without really knowing what the legislature meant by "reasonable particularity."

As a federal court in the Southern District of California recently pointed out, the legislative history behind § 2019(d) offers some guidance in determining the principles behind the statute. In *Computer Economics, Inc. v. Gartner Group, Inc.*, 50 F. Supp. 2d 980 (S.D. Cal. 1999), the court addressed the issue of whether § 2019(d) applies to federal courts following California trade secret law. The court, after examining § 2019(d)'s legislative history, determined that the statute is tied up with California's substantive trade secret law.

The court first noted that § 2019(d) was intended to codify dicta from the pre-UTSA trade secret decision in *Diodes, Inc. v. Franzen*, 260 Cal. App. 2d 244 (1968). Although that decision's holding addressed the issue of whether plaintiff, who alleged trade secret misappropriation, had pled misappropriation sufficiently to avoid a demurrer, the court stated in dicta that plaintiffs must identify their alleged trade secrets with greater specificity before obtaining discovery. In particular, the court stated that "the complainant should describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons who are skilled in the trade and to permit the defendant to ascertain at least the boundaries within which the secret lies." *Id*. at 253.

The court also found instructive a legislative memorandum that was passed among state assembly members before the enactment of California's version of the UTSA. That memorandum expressed concern that "[o]ne area not addressed by the Uniform Act is the area of plaintiff's abuse in initiating trade secret lawsuits for the purpose of harassing or even driving a competitor out of business by forcing a competitor to spend large sums in defending unwarranted litigation . . . Furthermore, by not informing the defendant with any degree of specificity as to what the alleged trade secrets are, the defendant may be forced to disclose its own business or trade secrets, even though those matters may be irrelevant, and the defendant may not learn the exact nature of the supposedly misappropriated trade secrets until the eve of trial." *Computer Economics*, 50 F. Supp. 2d at 985 n.6 (quoting Memorandum from Messrs. John Carson and Greg Wood to Assemblyman Harris re: Assembly Bill 501).

After examining the statute's legislative history, the *Computer Economics* court found that § 2019(d) serves four purposes: First, it discourages the filing of meritless and harassing trade secret complaints. Second, it prevents a plaintiff from using litigation and discovery as a means of gaining access to a competitor's confidential information. Third, it helps both the court and the defendant clarify the permissible scope of discovery. Fourth, it streamlines the issues so that a defendant can develop defenses early in the litigation, rather than being forced to wait until the eve of trial. *Id*. at 985.

It is likely that concerns such as these led to the enactment of § 2019(d) concurrent with the adoption of the UTSA. The Diodes language taken in conjunction with the statutory purposes recognized in *Computer Economics* offers litigants and courts some guidance as to the purpose of the "reasonable particularity" requirement, but it does not address the ultimate issue that faces litigants and courts: just how specific must a plaintiff's description be to satisfy the "reasonable particularity" requirement? The absence of reported state court case law is likely due to the nature of the statute as a discovery procedure. Because Superior Court rulings where § 2019(d) issues are litigated and resolved are not published in official or unofficial reporters, judges' reasoning as to whether plaintiffs have satisfied the statute's requirements are lost.

Case law from other jurisdictions, applying common law rules that are similar to § 2019(d), offers some additional guidance as to the meaning of the "reasonable particularity" requirement. Delaware, for instance, has a common law rule requiring plaintiffs alleging trade secret misappropriation to identify the alleged trade secrets at issue with "reasonable particularity." *See, e.g., Leucadia, Inc. v. Applied Extrusion Technologies*, 755 F. Supp. 635 (D. Del. 1991); *Engelhard Corp. v. Savin Corp.*, 505 A.2d 30, 33 (Del. Ch. 1986); *Magnox v. Turner*, 1991 Del. Ch. LEXIS 140 (May 15, 1991). In *Magnox*, the court rejected as insufficiently general plaintiff's statement that defendant's "knowledge of Magnox's confidential, proprietary information about customer specifications put him in the unique position of knowing which competing products to offer . . . customers." *Id*. Similarly, a Minnesota federal district court recently noted that "[o]rdering the listing of trade secrets at the outset of the litigation is a common requirement." *Porous Media Corp. v. Midland Brake Inc.*, 187 F.R.D. 598, 600 (D. Minn. 1999). There, the court found that general references to manufacturing processes and product designs, even for specifically identified products, were not sufficiently specific to entitle plaintiff to discovery.

However, even this limited case law from outside of California addresses only what does *not* satisfy the "reasonable particularity" requirement, rather than establishing guidelines as to what does satisfy § 2019(d). Because these determinations often rest on fact-specific grounds, it is difficult for litigants and courts to extrapolate a standard for what is reasonably particular. Until the legislature clarifies the meaning of § 2019(d), this situation is unlikely to change and protracted, costly court battles as to whether plaintiffs have satisfied the statute's requirements are likely to continue.

Until that time, however, litigants should look to the *Diodes* dicta and the legislative purpose of § 2019(d) when attempting to satisfy the statute's requirements. Parties should first agree upon a protective order so that plaintiffs may identify the alleged trade secrets to defense counsel. In order to avoid a protracted discovery dispute, plaintiffs should thoroughly investigate their claims and attempt to identify the trade secrets that they believe were misappropriated with sufficient detail to allow one who is skilled in the relevant technology to distinguish trade secrets from matters of general knowledge. This step will only help plaintiffs in the long run, as they bear the ultimate burden of proving the existence of a trade secret. For instance, if the alleged trade secret is a manufacturing process for a widget, plaintiffs should avoid catch-all designations such as "manufacturing process." Instead, they should identify each step of the process that they allege constitutes a trade secret under § 3426. When possible, plaintiffs should reasonably tailor their discovery requests to the categories identified.

Similarly, defendants should not abuse § 2019(d) by refusing to respond to discovery requests even where plaintiffs have identified details that are not generally known. Retaining an independent expert early in the case will allow defendants to make informed

decisions as to whether plaintiffs have satisfied § 2019(d)'s requirements. Where defendants believe that plaintiffs' designations are overly broad, they should inform plaintiffs of their reasons and request the details that would enable them to determine whether plaintiffs have identified trade secrets. Both parties will be well served by attempting to resolve the dispute through a meet and confer process, rather than burdening the court.

## Lessons Learned From the Avant! Criminal Trade Secrets Case

Donald Searles (dsearles@fenwick.com)

In a triumph of perseverance, the Santa Clara District Attorney's Office recently claimed victory in the landmark Avant! trade secrets case, *People v. Avant!*, No. 210570, (Sup. CT. 2061). After one criminal complaint, two indictments, three attempts to have the District Attorney's Office disqualified from handling the case, four years of pre-trial maneuvering, and five different judges, on May 22, 2001, Avant! Corp. and seven of its current and former executives entered no contest pleas to charges of securities fraud and misappropriating trade secrets from its competitor, Cadence Design Systems, Inc. Under the terms of the plea agreements, Avant! agreed to pay a $27 million fine and its President and CEO, Gerry Hsu, agreed to pay a $2.7 million fine. The remaining defendants agreed to pay an additional $5 million in fines and face possible incarceration. In addition, Avant! was ordered to pay almost $200 million in restitution. Given the difficulties in reaching this conclusion, however, it remains to be seen whether other companies are willing to follow Cadence's lead and refer trade secret thefts for criminal prosecution.

The Avant! case first came to the public's attention in late 1994, when police raided the Los Gatos home of Mitch Igusa, a former Cadence engineer who was alleged to have received secret payments in exchange for providing Cadence's trade secrets to Avant! Among the more damning pieces of evidence collected by the District Attorney's Office in Igusa's home and elsewhere were: the source code of Avant!'s ArcCell place-and-route software (used in the design of computer chips), which was identical to that of Cadence; an electronic footprint showing that a Cadence employee had e-mailed six megabytes of source code to his private account before joining Avant!; copies of Cadence's software with the copyright notices removed; and a "Resignation Q & A" containing scripted responses for defendants' use during their exit interviews with Cadence.

### The Pros and Cons of Referring A Case for Criminal Prosecution

Although this evidence made for a compelling case under California's criminal trade secrets statute, Cal. Penal Code § 499c (West 2000), the resulting judicial paralysis is likely to give future corporate victims pause before turning to law enforcement for protection of their

trade secrets. Before deciding on turning over a trade secrets case to a county prosecutor or the U.S. Attorney's Office, the corporate victim should carefully consider the pros and cons involved.

The most obvious advantage to criminal prosecution over civil litigation is the cost to the victim. Particularly where the alleged perpetrator is without sufficient funds to pay a meaningful damages award, criminal prosecution may be the most expedient means for punishing the wrongdoer. In addition, law enforcement agencies have numerous investigative tools not available to private litigants, including the ability to compel testimony from recalcitrant witnesses, use search warrants to seize evidence without prior notice, and surreptitiously record conversations with potential suspects. Depending on the need for such measures, referring the matter for criminal prosecution may be the only means to obtain the necessary evidence to prove the theft and the identity of the thief.

As Cadence discovered, however, there are costs involved in referring a matter for criminal prosecution. One of the most significant costs is the victim's loss of control over the process, including settlement. Plus, the looming presence of a criminal case makes it far less likely that defendants will agree to any civil resolution. Moreover, global resolutions of both criminal and civil charges are extraordinarily difficult to negotiate, as the prosecutor is generally unwilling to risk the appearance that he or she is improperly using the threat of criminal charges to facilitate the resolution of a civil case.

Furthermore, a criminal prosecution does not obviate the need for filing a parallel civil proceeding, since California's criminal trade secret law does not provide for immediate injunctive relief. Cal. Penal Code § 499c. Civil discovery, however, is likely to be stayed indefinitely, as it was in *Avant!*, since Fifth Amendment self-incrimination issues make it difficult for defendants to defend the civil case while facing indictment. *See, e.g., Pacers, Inc. v. Superior Court*, 162 Cal. App. 3d 686 (1984) (authorizing stay of civil discovery pending expiration of criminal statute of limitations).

In light of a criminal defendant's right to a public trial, expansive criminal discovery rights, and constitutional guarantees of compulsory process and right of confrontation, it is difficult to protect a company's trade secrets from disclosure in a criminal prosecution. *See e.g.*, Cal. Evid. Code § 1061 (West 2000), setting forth procedure for obtaining an order protecting the confidentiality of trade secrets in a criminal case. Since the government is required to prove every element of the offense beyond a reasonable doubt, each element will be vigorously contested, resulting in a painstaking examination of whether the allegedly-stolen technology constitutes a trade secret. This examination presents a criminal defense lawyer with the opportunity to raise numerous defenses that make it difficult for a jury to unanimously agree on a verdict. For example, it may be possible to argue that the alleged trade secrets were reverse engineered from products obtained by proper means, which would be a complete defense to a claim of trade secret misappropriation. *See, e.g., Sony*

*Computer Entertainment v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000). It may also be possible under the equitable defenses of unclean hands and laches to place into issue the company's motivations in forwarding the case for criminal prosecution, and thereby obtain discovery of internal memoranda that might otherwise be protected under the attorney-client privilege and work product doctrine. *See, e.g., Unilogic, Inc. v. Burroughs Corp.*, 10 Cal. App. 4th 612 (1992), permitting an unclean hands defense to be asserted affirmatively against a legal claim for damages.

**The Unresolved Legacy of Eubanks**

Assuming the decision has been made to refer a trade secrets theft for criminal prosecution, the victim must not become overly involved in the prosecutor's investigation, as it may result in the prosecutor's disqualification. In *People v. Eubanks*, 14 Cal. 4th 580 (1996), the California Supreme Court disqualified the Santa Cruz District Attorney from the Borland/Symantec criminal trade secrets case after Borland, the victim, paid a $13,000 bill already incurred by the District Attorney's office in hiring a computer expert to conduct a portion of the investigation. The Supreme Court found that Borland's financial assistance resulted in a potentially disabling conflict of interest since "the private financial contributions were of such a nature and magnitude likely to put the prosecutor's discretionary decision making within the influence or control of an interested party." *Id*. at 599.

In *Avant!*, the defense repeatedly sought to recuse the District Attorney's Office under Eubanks since the prosecutor relied extensively on the research and data generated by Cadence's experts in its own civil case. In addition, Cadence also loaned the prosecutors a computer workstation to process information. The District Attorney's Office successfully fought these challenges on the theory that Cadence was not paying off a debt "already incurred." But shortly before the *Avant!* defendants entered their no-contest pleas, the California Supreme Court requested that the Office respond to the defense's writ, raising the specter that the Court was not satisfied with the narrow interpretation of Eubanks given by the lower courts.

**Avoiding Criminal Exposure**

A company accused of trade secret theft should be prepared for such charges. The presence of "illegal" data within a company is like a virus that quickly spreads. As Avant! found, a company's very existence can be challenged as an ongoing criminal enterprise based on its alleged possession of another company's trade secrets. To protect against such an accusation, and the potentially dire consequences of a criminal prosecution, every company should have a detailed compliance plan. Such a plan will enable a company found in possession of unauthorized secrets to argue that it was victimized by a rogue employee. *See, e.g.*, United States Sentencing Commission, *Guidelines Manual*, §8A1.2 (Nov. 1998).

Finally, a company facing an accusation of trade secret theft should respond carefully. Avant!'s executives issued various seemingly-innocuous denials of wrongdoing, including the following:

- "The Company's products are based on the Company's proprietary architecture and technology, which provide a breadth of automated IC physical design capabilities."

- "The Company believes its products and trademarks do not infringe upon the proprietary rights of third parties."

- "Avant! has never made any improper use of Cadence technology, stolen any purported trade secrets, infringed any copyrighted material or engaged in any wrongful acts toward Cadence."

The Santa Clara District Attorney's Office, however, took the position that each of these statements was false, in that Avant!'s executives allegedly knew that its products were based on trade secrets that had been stolen from Cadence, and used these statements as the basis for the securities fraud charges.

In conclusion, criminal enforcement, under Cal. Penal Code § 499c represents an important weapon in the fight against trade secret theft. But, as *Avant!* teaches, this remedy must be used carefully and with a full awareness by the victim of its potential advantages and disadvantages.

## Quick Updates

**Reproduction in Electronic Media Not A Eevision Permitted by Section 201 (c)**
As we reported in the last *IP Bulletin*, the Supreme Court agreed to review the decision of *Tasini v. New York Times Co.*, 206 F.3d 161, (2d Cir. 1999). On June 25, 2001, the United States Supreme Court ruled that publishers violate the copyright of freelance writers when they reproduce the writers' works in electronic media unless the publishers have negotiated and paid for that right because such reproduction is not a revision of the original work as encompassed by Section 201 (c) of the Copyright Act. *New York Times Co. v. Tasini*, 121 S. Ct. 2381 (2001), Slip Op. No. 00-201, June 25, 2001. In holding that the electronic reproduction of the writers' articles is not a reproduction or revision encompassed by Section 201 (c), the Supreme Court explained that such electronic reproduction differs from reproduction in microfiche or microfilm format in that "each article appears as a separate item within the search result." *Id*. at 14. Addressing the principle of media neutrality, the Court stated that, unlike the situation where a collective work has been reproduced in microfiche or microfilm, there is no conversion of the entire collective work in intact form when it is reproduced in an electronic database since such databases permit the storage and retrieval of articles individually, apart from the collective work in which they originally appeared. *Id*. at 16-18. Such a system "effectively overrides the Author's right to control the individual reproduction and distribution of each Article." *Id.* at 18. An agreement whereby authors permit publishers to reproduce their articles electronically prevents this problem.

**Caveat E-Retailer**

In two separate decisions, the United States District Court for the Southern District of New York has ruled that New York's long arm statute permits jurisdiction over out-of-state Web site operators and e-retailers.

In *Starmedia Network Inc. v. Star Media Inc.*, 2001 U.S. Dist. LEXIS 4870 (S.D.N.Y. April 23, 2001), plaintiff, based in New York, sued defendant, based in Washington, on the basis that defendant's use of the starmediausa.com domain infringed plaintiff's rights in its trade name. The defendant had no customers in New York, and argued that the court therefore had no jurisdiction over it. The court held that New York's long-arm statute reached the defendant because it should have expected that its acts would have consequences within New York State, and further, that it benefits from interstate or international commerce. In holding that jurisdiction was proper, the court noted that the defendant's Web site was clearly commercial. The fact that the site allowed for e-mail exchanges and the access of confidential information was sufficient for jurisdiction to be proper, even though it did not allow for actual sales over the Internet.

In another decision, the same court ruled that jurisdiction was proper over an Arizona defendant on the basis of a single electronic sale from the defendant to plaintiff's investigator based in New York. In *Mattel, Inc. v. Adventure Apparel*, 2001 U.S. Dist. LEXIS 3179 (S.D.N.Y. March 15, 2001), plaintiff Mattel sued an Arizona man who had registered and was using the domain names, "barbiesbeachwear.com" and "barbiesclothing.com." Based in Tucson, the defendant sold swimwear and tanning sessions. Plaintiff Mattel, maker of, and owner of the registered trademark for, the Barbie® doll, sued the defendant retailer for trademark infringement, among other causes of action. Plaintiff's investigator purchased hosiery from the defendant by accessing one of defendant's Web sites through defendant's barbiesbeachwear.com address. The court held that this single sale, defendant's only contact with the forum state, was sufficient to establish jurisdiction over the defendant under New York's long-arm statute.

Similarly, the U.S. District Court for the Northern District of Illinois recently held that its jurisdiction over a defendant based in Hawaii was proper even though that defendant had only engaged in a single Internet transaction with an Illinois customer. In *Ty, Inc. v. Baby Me Inc.*, 2001 U.S. Dist. LEXIS 5761 (N.D. Ill. April 20, 2001), plaintiff Ty, the manufacturer of Beanie Babies stuffed animals sued the defendant, a retailer based in Hawaii that makes Baby Me Bears and sells them both at retail in Hawaii and over the Internet, for copyright infringement and other causes of action. Defendant sought dismissal on the basis that the court lacked personal jurisdiction. The court held jurisdiction was proper because the defendant had established a Web site clearly intended to enable business with customers throughout the United States, and had such contact with a purchaser based in Illinois.

**Enabling Disclosure Demonstrates that Software Invention is "Ready For Patenting" Despite Actual Code Being Not Yet Written for Purposes of Assessing On-Sale Bar**

In *Robotic Vision v. View Engineering*, 249 F. 3d1307 (Fed. Cir. 2001) the Federal Circuit found a patent claim invalid due to the on-sale bar. The Robotic Vision ("Robotic") patent claims a method of scanning integrated circuit devices. The method reduces overall scanning times as compared to prior art techniques. The application for the patent was filed on June 24, 1992, thereby establishing a critical date of June 24, 1991 for the purposes of the on-sale provision of the patent statute—35 U.S.C. § 102(b). This provision states that a person is entitled to a patent unless the invention was on sale in this country more than one year prior to the filing date of the application. The Supreme Court recently held in *Pfaff v. Wells Elec., Inc.*, 525 U.S. 1094 (1999) that the on-sale bar provision applies when the claimed invention is both: (1) the subject of a commercial offer for sale; and (2) "ready for patenting" before the critical date.

Robotic filed suit alleging that View Engineering ("View") scanning machines infringed the patent. At trial, the district court found the patent to be invalid because the claimed invention was both the subject of a commercial offer for sale and "ready for patenting" before the critical date, thereby satisfying the *Pfaff* test. On appeal, the sole issue was whether Robotic's patented method was "ready for patenting" prior to the critical date. The Federal Circuit noted that an invention may be shown to be ready for patenting in at least two ways: 1) by showing "proof of reduction to practice before the critical date;" or 2) by showing that before the critical date the "inventor had prepared drawings or other descriptions of the invention that were sufficiently specific to enable a person skilled in the art to practice the invention."

The relevant facts were that, before June 1991, one of the inventors explained the invention to a programmer. Based on the description given by the inventor, the programmer wrote the software necessary to implement the invention. The Federal Circuit therefore concluded that the inventor's explanation was sufficiently specific to enable a person skilled in the art (the programmer) to practice the claimed invention. The fact that the software was not actually completed until after the critical date was found to be irrelevant in light of the inventor's enabling disclosure. As the invention was both the subject of a commercial offer for sale, and ready for patenting before the critical date, the court affirmed the district court's finding of invalidity.

Interestingly, Robotic argued that the inventor's disclosure to the programmer was not sufficient because the inventor expressed skepticism as to whether the invention would work for its intended purpose. The Federal Circuit disagreed, stating that there is no requirement that the inventor have "complete confidence" his invention will work for its intended purpose.

**E-Mail Privacy—The Regulation of Spam**

To date, sixteen states have enacted legislation regulating unsolicited commercial electronic mail, known in the industry as "UCE" and to the public as "spam." The problem for those who use e-mail as a marketing tool has been not only trying to comply with these various state laws, but also trying to comply with a handful of related laws at the federal and state level which affect how e-mail can be used for commercial purposes. California's 1998 statute, for example, is similar to "spam" legislation in other states; it requires marketers to include the abbreviation "ADV" (or, for adult materials, "ADV:ADLT") in the subject line of every unsolicited message and to provide recipients with an opt-out, toll-free phone number or valid return e-mail address. Cal. Bus. & Prof. Code § 17538.4 (Deering 2001). Some states have enacted more stringent regulatory schemes; Delaware, for example, prohibits any entity (including out-of-state marketers) from sending spam to a Delaware resident. These statutes are facing mixed response by the courts. In June 2000, a state court judge ruled that California's law was unconstitutional because it placed excessive restrictions on interstate trade, but on June 7, 2001, the Washington Supreme Court unanimously upheld that state's statute on identical grounds. Wash. Rev. Code Ann. § 19.190 (2001).

Given the varied level of restrictions in state laws, the uncertain judicial reception of such laws, as well as the assortment of various related federal and state laws, industry groups and privacy advocates alike have called for comprehensive federal legislation which would clarify the area. While several bills have been proposed in recent years, none has passed.

Most recently, the best prospect for comprehensive legislation was the "Unsolicited Commercial Electronic Mail Act of 2001," introduced by Representatives Heather Wilson of New Mexico and Gene Greene of Texas, and which had garnered bipartisan support from members of Congress, including California's Gary Miller. "Unsolicited Commercial Electronic Mail Act of 2001," H.R. 718, 10th Cong. (1st Sess. 2001). Despite solid initial support, companies and industry groups such as Amazon.com, the National Retail Federation, the Direct Marketing Association, and consortiums representing banks and securities firms soon lined up to oppose the legislation. Meanwhile, consumer and privacy groups argued that the bill, which prohibited class action lawsuits and declined to adopt an "opt-in" mechanism similar to that of the anti-junk fax Telephone Consumer Protection Act of 1991 ("TCPA"), was too weak. "Telephone Consumer Protection Act of 1991," 47 U.S.C. § 227 (2001).

The original text of the bill:

- established criminal penalties when messages were sent containing fraudulent routing information or headers;
- made it illegal to send unsolicited e-mail to consumers who had asked to be removed from a distribution list;
- empowered internet service providers to block all messages from senders identified as "spammers";

- allowed consumers to sue companies that ignored their requests to be removed from distribution lists; and
- set a $500 per message penalty for each unsolicited e-mail sent to an individual who had asked not to receive such messages.

The House Judiciary Committee's amendments eliminated all but the first of these provisions, reducing the bill's reach to technical fraud, and added a provision directing the U.S. Attorney General to order warning labels for e-mails containing pornographic material.

There is no word as to when the legislation will come up for a full vote in Congress. In March 2001, an identical version of the legislation proposed by Representatives Wilson and Greene was introduced in the Senate by Montana's Conrad Burns as the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001," or the "CAN SPAM Act of 2001"; it remains to be seen whether the recent change in control of the Senate will result in inconsistencies between the two bills. "CAN SPAM Act of 2001," S.630, 107th Cong. (1st Sess. 2001). Until such a time as comprehensive spam legislation is enacted at the federal level, the regulation of spam will continue to be an awkward combination of state and related federal laws.

## Intellectual Property Bulletin Editorial Staff

**Summer 2001**

**Editor**
John T. McNelis

**Assistant Editors**
Brian M. Hoffman
Barbara Nesbet

**Article Contributors**
Tyler Newby
Donald W. Searles
Scott Gattey

**Update Contributors**
Neil F. Maloney
Susan M. Marsh
Daniel J. O'Rourke