FENWICK & WEST LLP

Intellectual Property Bulletin

Fenwick & West LLP — Spring 2000

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.

The contents of this publication are not intended, and cannot be considered, as legal advice or opinion.

FENWICK & WEST LLP

Intellectual Property Bulletin

Spring 2000

Table of Contents

U.S. Encryption Export Regulations Enter the 21st Century

Edward J. Radlo (eradlo@fenwick.com)

On January 10, 2000, the U.S. Commerce Department issued an “interim final” rule substantially liberalizing the U.S. government’s restrictive policy concerning the export and re-export of encryption commodities and software. While the government had issued an announcement in September 1999 stating that the encryption export rules would be loosened, the draft rules, which circulated between September 1999 and January 2000, were disappointing to industry and civil liberties activists who had been fighting for years to get these rules liberalized. However, as discussed below, the “interim final” rule resolved a number of issues in favor of the industry/civil liberties position.

Encryption Levels

Generally speaking, the government’s new encryption export policy recognizes three levels of encryption.

The first level is an encrypted message itself. The government does not place any restrictions upon exporting an encrypted message outside of the United States or Canada.

The second level comprises encryption software and encryption commodities. The government places three layers of restriction upon this level: (a) prior screening by the Commerce Department; (b) regulating, and in some cases prohibiting, exports of certain encryption items to government end-users; and (c) imposing post-export reporting requirements.

The third level comprises encryption that has a “multiplier effect,” *i.e.*, encryption items that can spawn additional encryption items. Examples of such multiplier-effect encryption items are: (a) items that are exported to a foreign telecommunications company (telco) or to a foreign Internet service provider (ISP);(b) exports of open cryptographic interfaces; (c) exports of encryption tool kits; and (d) exports of technical assistance involving encryption. Generally speaking, the government places greater restrictions on the export and re-export of items within level three than for items within level two.

Cryptography

As before, the government does not place restrictions upon authentication cryptography and does not place restrictions upon the import of cryptography into the United States. Also, the government does not impose restrictions upon the use of cryptography within the United States; however, the government continues to press for the escrow of encryption keys, with the government having the ability to recover such keys under certain circumstances, such as upon the presentation of a search warrant.

Export of Retail Encryption Products

Perhaps the biggest liberalization in the new rule is that a U.S. entity is now allowed to export and re-export, to almost any end-user, encryption commodities, encryption software and encryption components that have been reviewed by the U.S. government prior to export and that have been classified as "retail" encryption items. The significant change is that the export is not conditioned upon the size of the encryption key or the type of encryption, as it was under the prior regulations. The only end-users prohibited from receiving "retail" encryption items are individuals specifically prohibited by the U.S. government and entities in countries where the government has determined that terrorism is fomented.

The definition of "retail" is of course very important. "Retail" is defined in the regulations as being "generally available to the public" by certain specifically enumerated means plus satisfying each of the following four requirements: (a) the cryptographic functionality cannot be easily changed by the user; (b) the exported items do not require substantial support for installation and use; (c) the cryptographic functionality has not been modified or customized to customer specification; and (d) the exported items are not network infrastructure products, such as high-end routers or switches designed for large volume communications.

The regulations state that retail encryption products include the following: (a) general purpose operating systems and their associated user-interface client software; (b) general-purpose operating systems with embedded networking and server capabilities; (c) nonprogrammable encryption chips; (d) chips that are constrained by design for retail products; (e) low-end routers, firewalls and networking or cable equipment designed for small office or home use; (f) programmable database management systems and associated application servers; (g) low-end servers and application-specific servers including client-server applications, *e.g.*, Secure Socket Layer (SSL-based applications) that interface directly with the user; and (h) encryption products distributed without charge or through free or anonymous downloads.

The regulations further state that the following types of products are also deemed retail encryption products: (a) encryption products and network-based applications that provide functionality equivalent to other encryption products classified as "retail"; (b) finance-specific encryption commodities and software of any key length, restricted by design and used to secure financial communications, such as electronic commerce; and (c) 56-bit products with key exchange mechanisms greater than 512 bits and up to and including 1024 bits, or equivalent products not classified as mass market.

Exporters of retail encryption commodities and software must still comply with postexport reporting requirements and face severe criminal, civil and administrative penalties for failure to comply with the regulations. The reporting requirement is biannual and is made to the Bureau of Export Administration (BXA) within the U.S. Commerce Department.

Export of Non-Eetail Encryption Products

If the encryption commodity or software is not classified as "retail" after a one-time government review, the product may nevertheless be exported to any nongovernment end-user (with the usual provision concerning terrorist states). Again, this is true regardless of the key length or type of encryption product. The new regulations define "government end-user" as: (a) any foreign central, regional or local government department, agency or other entity performing governmental functions, including governmental research institutions, governmental corporations or their specific business units that are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List; and (b) international governmental organizations. The term "government end-user" expressly excludes utilities (such as telcos and ISPs), banks and financial institutions, transportation agencies, broadcast or entertainment agencies, educational organizations, civil health and medical organizations, retail or wholesale firms and manufacturing or industrial entities not engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.

Export to Foreign Telcos and ISPs

The regulations have special rules for exports made to a foreign telco or ISP. The regulations provide that when the telco or ISP is providing application-specific e-commerce services and PKI (public key infrastructure) encryption services specifically for government end-users (and not general-purpose services where a foreign government happens to be one of many end-users), a license must first be obtained from the BXA.

Export of Encryption Source Code

In another liberalization, encryption source code considered "publicly available" may be exported or re-exported to any end-user without prior review and classification, provided that the exporter submits to the BXA, at the time of export, written notification of the Internet location of the source code or a copy of the source code. This special rule further states that one may not knowingly avail oneself of this rule to export to one of the prohibited terrorist countries, but a general posting of such publicly available source code on the Internet, where the source code may be downloaded by anyone, does not, by itself, constitute a prohibited export to a terrorist country.

Software (source code or object code) that does not meet the definition of "publicly available," or that is subject to an express agreement for the payment of a licensing fee or a royalty for commercial production or sale of any product developed with the source code, generally remains under the previously existing rule, under which such software may be posted on the Internet subject to address checking, notice and affirmative acknowledgement requirements.

Export to Foreign Subsidiaries

Another significant liberalization in the new regulations is a provision that permits foreign subsidiaries of U.S. companies to freely receive encryption products and encryption technical assistance without a prior technical review by the government. Such transfers include "deemed exports," which occur when encryption items pass within the United States from U.S. nationals to foreign nationals. However: (a) any items developed by the U.S. company for sale or retransfer outside of the U.S. company are subject to review and classification by the Commerce Department; (b) foreign companies with U.S. subsidiaries must apply for the very cumbersome "encryption licensing arrangement" to obtain treatment equivalent to that extended to foreign subsidiaries of U.S. companies; and (c) export of technical assistance pertaining to encryption technology still generally requires a license from the U.S. government.

Other Provisions

Mass-market encryption items having key lengths of 64 bits or less are now made exempt from the reporting requirements in most cases. This rule ensures compliance with the agreement reached within the Wassenaar Arrangement in December 1998.

Other areas of liberalization include the following: (a) a simplified means for an exporter to upgrade a product where the only change is an increase in key length; (b) a provision that places a fixed time limit on the period within which the government must act on a classification request; and (c) certain grandfathering provisions.

The government remains concerned about "open cryptographic interfaces," which are defined as mechanisms designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, *e.g.*, the manufacturer's signing of cryptographic code or proprietary interfaces.

A license is required for "open cryptographic interfaces" unless the source code is publicly available, or unless the export is to a subsidiary of a U.S. company.

Conclusion

As can be seen from the above, the new regulations remove some of the previous restrictions on the U.S. cryptography industry but are needlessly complicated. The next few months will witness attempts to further simplify U.S. encryption export policy.

Ninth Circuit Clarifies Scope of Fair Use of Computer Code

Robert Brownstone (rbrownstone@fenwick.com)

On February 10, 2000, the Ninth Circuit Court of Appeals held that a software manufacturer's "reverse engineering" of a copyrighted product to create an emulating, but noninfringing, final product was a protected fair use under 17 U.S.C. § 1707. *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F. 3d 596 (9th Cir. 2000). The decision reversed the trial court's April 20, 1999, grant of a preliminary injunction in favor of plaintiff Sony Computer Entertainment, Inc., and its subsidiary Sony Computer Entertainment America (collectively "Sony") and against defendant Connectix Corporation ("Connectix").

As characterized by the appellate court, this case implicated the tension in software copyright cases between publicly accessible function and protected expression. 203 F. 3d at 598. The underlying lawsuit involved Sony's attempt to keep its gaming console, the PlayStation, as the exclusive means for playing PlayStation games. Sony has a copyright on the console's firmware. The firmware is essentially the equivalent of an operating system that resides in a read-only memory (ROM) in the console and defines a basic input-output system (BIOS) for the PlayStation.

In July 1998, Connectix—a developer, manufacturer and marketer of computer software—began developing a PlayStation emulator called Virtual Game Station (VGS). VGS, which Connectix created using a purchased PlayStation console, allows PlayStation games to be executed and played on a standard personal computer.

In September 1998, while developing VGS, Connectix obtained a meeting with Sony and asked for technical assistance—which Sony declined. A few months later, on January 5, 1999, at the Macworld Expo, Connectix announced that it had completed the Apple Macintosh version of the VGS product.

Sony quickly responded on January 27, 1999, by suing Connectix in the United States District Court for the Northern District of California. The complaint alleged copyright infringement, trademark dilution and various other causes of action. At the time the lawsuit was filed, Connectix was marketing a Macintosh version of its VGS software, but had not yet developed VGS software for Microsoft Windows. *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 48 F. Supp. 2d 1212, 1216 (N.D. Cal. 1999).

Two months into the lawsuit, Sony moved for a preliminary injunction on the copyright and trademark claims. In a decision by Judge Charles A. Legge, the trial court found that "to develop a PlayStation emulator, Connectix needed to emulate both the PlayStation hardware . . . and the firmware (the Sony BIOS)." 48 F. Supp. 2d at 1216. He also found that it was:

> undisputed that the early version of VGS contained the complete, unchanged Sony BIOS. Prior to the meeting with Sony, Connectix had not taken any steps to develop its own BIOS. The evidence show[ed] that Connectix did not begin developing its own BIOS until after Sony had declined Connectix' request for technical assistance, sometime in October 1998. As its final step in the VGS development, Connectix replaced the Sony BIOS code with its own BIOS code. *Id*.

Thus, even though VGS ultimately did not contain any of Sony's copyrighted material, it contained a functional copy of the BIOS code. The trial court characterized Sony's theory as "intermediate infringement [in] two distinct forms," namely: (1) the repeated duplication of Sony's entire BIOS code to develop its own program; and (2) the disassembly of Sony's BIOS "to develop its own VGS BIOS by gradually replacing elements of Sony's code with its own." *Id*. at 1217.

In ruling on the preliminary injunction request, the trial judge held that "Sony ha[d] shown a high probability of success" on its claim. *Id*. at 1221. In particular, he ruled that: Connectix had "admit[ted] to copying and using the entire Sony BIOS [which was] unlawful copying under the Copyright Act," *Id*. at 1218; and all four factors of the "fair use" defense of 17 U.S.C. § 1707 favored Sony, *Id*. at 1218-21. He also found a likelihood of success on the trademark claim. Thus, Judge Legge granted the motion, not only enjoining the sale of VGS for Macintosh and Windows but also enjoining Connectix from copying the Sony BIOS code in the development of other VGS products. *Id*. at 1224.

Connectix appealed the decision to the Ninth Circuit. A three-judge appellate panel reversed, directing that the injunction be dissolved. The appellate court sanctioned Connectix's development of VGS as a valid "process of reverse engineer[ing of a] copyrighted product to gain access to [its] functional elements." 203 F. 3d at 602. In particular, the higher court ruled that:

> [t]he object code of a program may be copyrighted as expression, 17 U.S.C. §102(a), but it also contains ideas and performs functions that are not entitled to copyright protection. See 17 U.S.C. §102(b). Object code cannot, however, be read by humans. The unprotected ideas and functions of the code therefore are frequently undiscoverable in the absence of investigation and translation that may require copying the copyrighted material. *Id*.

Thus, the court found that the intermediate copies made by Connectix in the reverse engineering process "were protected fair use . . ." *Id*. at 599. In assessing likelihood of success under the four pertinent statutory fair use factors, the Ninth Circuit found that three factors ("nature of the copyrighted work," "purpose and character of the use" and "effect of the use upon the potential market") favored Connectix and that the only factor that favored Sony ("amount and substantiality of the portion used") was generally not a weighty factor. *Id*. at 606.

As to nature of the copyrighted work, the court found that there were “unprotected functional elements” to which Connectix could not have obtained access without reverse engineering and copying. *Id.* at 604. As to purpose and character of use, the court found that VGS was “modestly transformative [in that] it create[d] a new platform” on which to play Sony’s games. *Id.* at 606. That transformative nature also persuaded the court to rule for Connectix on the “effect on the market” factor. *Id.* at 607.

The Ninth Circuit also reversed the district court’s finding that Sony was likely to show that VGS tarnished the PlayStation trademark. The court therefore dissolved the injunction and sent the case back to the district court.

Significantly, the Sony decision also essentially invited Sony to replace its copyright claim with a patent infringement claim. In particular, the court stated: “If Sony wishes to obtain a lawful monopoly on the functional concepts in its software, it must satisfy the more stringent standards of the patent laws.” *Id*. at 605. Just four days after that invitation, on February 14, Sony responded by filing a new Northern District of California lawsuit against Connectix. This time Sony alleged that Connectix infringed 11 patents on various PlayStation audio and video components.

In the interim, Connectix has started shipping the Macintosh and Windows versions of VGS. On February 10, the day of the Ninth Circuit decision, Connectix issued a press release announcing that the Macintosh version was ready for shipment and that online sales were commencing. On March 6, 2000, Connectix announced shipment of VGS for Windows PCs.

Quick Updates

Metallic Color of Platters Found Aesthetically Functional

Imitation shiny gold or silver serving platters are not protectable for their trade dress because the shiny gold or silver look is aesthetically functional. *Sabert Corp. v. Ullman Co.*, 53 U.S.P.Q.2d (BNA) 1597 (S.D.N.Y. 1999). A federal district court judge ruled that protecting a particular manufacturer’s use of silver and gold colors on its plastic serving trays would eliminate competition, because other manufacturers of the trays would be unable to use those colors to imitate the real metals. The products’ design was also not found to be sufficiently distinctive to merit trade dress protection.

Public Domain Movie Clip not Protected by Trademark Law

The owner of a 30-second movie clip of the Three Stooges that has fallen into the public domain could not use trademark law as a substitute form of protection for the expired copyright. *Comedy III Productions, Inc. v. New Line Cinema*, 53 U.S.P.Q.2d (BNA) 1858 (9th Cir. 2000). The trademark infringement claim was brought against New Line Cinema for its use of a film clip in the background of a movie. The plaintiff Comedy III Productions claimed trademark rights in the movie clip because it used the name, characters, likeness and overall act of the Three Stooges. The court rejected this argument on the ground that the movie clip was clearly covered by the Copyright Act and had fallen into the public domain. The Lanham Act could not be used to circumvent the copyright law. The court noted that had the defendant New Line Cinema used a likeness of the Three Stooges on t-shirts, or some other commodity, Comedy III Productions might have successfully brought a trademark infringement action.

Proposed California Bill Against Cybersquatting

A California bill (S. B. 1319) introduced by Senator Burton on January 3, 2000, would prohibit "cybersquatters" from reserving Internet domain names that use trademarks, service marks or names of famous people for their own profit. Unlike the federal bill, the California bill would protect a famous person even if her name were not a registered trademark. The California bill creates no financial remedies, but does include provisions for the cybersquatters to turn over the domain names to the proper owners. Domain name registrars would not be liable for the cyber-pirates' actions.

Corporate Director/Officers Can Be Held Personally Liable for Misappropriation of Trade Secrets

In *PMC, Inc. v. Kadisha*, 2000 Cal. App. LEXIS 178 (Ca. Ct. App. 2000) the Second District faced the issue of "whether, as shareholders, officers and directors of a corporation, defendants can be held personally liable for misappropriation of trade secrets, unfair competition, or interference with prospective economic advantage." The court held that "a corporate officer or director may be liable for an intentional tort if: (1) the officer or director purchased or invested in the corporation the principal assets of which were the result of unlawful conduct; (2) the officer or director took control of the corporation and appointed personnel to run the corporation which was engaging in unlawful conduct; and (3) the officer or director did so with knowledge or, with respect to trade secret misappropriation, when she or he had reason to know, of the unlawful conduct."

In the case, plaintiffs PMC and WFI sued officers and directors (who were also investors) of a newly formed rival corporation on the grounds of misappropriation of trade secrets including theft of customer lists, product specifications, and proprietary information. The defendants countered with a complete defense that they could not be liable for misappropriation of plaintiff's trade secrets. The defendants asserted that they did not direct any of their officers or employees to engage in any wrongful or unlawful activity and that they conducted an investigation upon receiving a cease and desist demand from the plaintiff. The trial court granted a summary judgment for the defendants, but the Second District reversed.

The Second District stated that "an officer or director will not be liable for torts in which he does not personally participate, of which he has no knowledge, or to which he has not consented [and while] the corporation itself may be liable for such acts, the individual officer or director will be immune unless he authorizes, directs, or in some meaningful sense actively participates in the wrongful conduct." However, a "corporate director or officer's participation in tortious conduct may be shown not solely by direct action but also by knowing consent to or approval of unlawful acts." Here, the evidence showed that the "defendants, in anticipation of enormous corporate and personal profit, knowingly invested at a bargain price in a corporation whose sole business assets consisted of stolen confidential information and processes, and subsequently controlled the entity which was engaging in unlawful conduct." In addition, there was evidence that the scope and results of defendants' investigation was questionable so as "to raise a triable issue whether, even if defendants did not know about the prior misconduct, they unreasonably took no action to prevent ongoing injury to [the plaintiffs]."

Circuit Court Addresses Presettable Levels or Threshold Values in Claim Construction

In *Vivid Technologies, Inc. v. American Science & Engineering, Inc.*, 200 F.3d 795 (Fed. Cir. 1999), the Federal Circuit was faced with interpreting a claim that included the terminology "presettable level." At issue was a patent for an x-ray radiation detection device used to detect threat items such as weapons and explosives. Unlike prior art x-ray detection devices, the patented item was able to display a scanned object as a color image.

The claims at issue included a means for displaying pixels in at least two different colors: the first color representing those pixels where radiation levels corresponded to a first presettable level; the second color representing those pixels where radiation levels corresponded to a second presettable level. The District Court concluded that the presettable level was a threshold level that was set by an operator before the object was scanned. On appeal, American Science argued that the claims did not limit when, where or how the presettable level of radiation was set. Instead, the levels must only be preset before the image was displayed.

The Federal Circuit agreed with the District Court's interpretation. The Federal Circuit began its analysis by reiterating that claims are construed as they would be understood by persons of skill in the art of the invention. When the meaning or scope of a claim is in dispute, the claim is read in light of the specification. Accordingly, the prosecution history is often helpful in understanding the intended meaning as well as the scope of technical terms.

The Federal Circuit focused on the specification that disclosed the use of a color look-up table that contained presettable reference levels, each level establishing the color to be displayed based upon a comparison with a level of radiation response for a scanned object.

Further, as disclosed, the intensity of the given color was a function of the amount by which the radiation response exceeds the presettable reference level. The specification only disclosed an embodiment wherein the look-up table was programmed with preset levels before the object was scanned. Although neither the specification nor the prosecution history suggested that these preset levels could be programmed into the look-up table after the radiation beam scanned the object but before the image was displayed, this embodiment was certainly feasible and should have been considered to be within the scope of the claims. The Federal Circuit, however, agreed with the District Court's claim interpretation in restricting the claims to the specific embodiment disclosed in the specification.

Intellectual Property Bulletin Editorial Staff

Spring 2000

Editor

John T. McNelis

Assistant Editors

Brian Hoffman
Diane L. Kort

Article Contributors

Edward J. Radlo
Robert Brownstone

Update Contributors

John Carr
Barbara Nesbet
Rajiv P. Patel
Susan Marsh