EMERGING CLAIM FORMATS FOR SOFTWARE INVENTIONS: VIRTUALLY EXTRATERRITORIAL REACH FOR U.S. PATENTS COVERING INTERNET-BASED INVENTIONS OR VIRTUALLY WORTHLESS?

§ 1.01 Introduction

This article will focus on emerging claim formats for software inventions. First, the article will provide a background describing commonly used intellectual property protection for software inventions, including copyright, trademark, trade secret and patent protection, including method, system, apparatus, Beauregard, and Lowry claim formats. The article will then focus on two emerging claim formats for software inventions: the propagated signal claim format and the product-by-process claim format. The article will then discuss the availability of these emerging claim formats as a means to protect software inventions in view of the U.S. Patent and Trademark Office's Examination Guidelines for Computer-Related Inventions, published opinions, and published commentary.

Second, the article will focus on practical issues that should be considered when utilizing these claim formats. For instance, the article will discuss the possibility that allowed claims in these emerging formats could be utilized to prohibit the "import" of data from Web sites located outside the U.S. via the Internet in a format covered by a propagated signal claim or a product-by-process claim. The article will also discuss the technical difficulties surrounding the enforcement of such claims (i.e., "how do you prohibit the 'import' of data on the Internet?"). Finally, the article will reach a conclusion as to whether the emerging claim formats will provide valuable protection that supplements the current commonly-used claim formats, or whether the legal and practical difficulties associated with the emerging claim formats outweigh their potential benefits.

§ 1.02 Background

[A] Current Non-Patent Protection Regimes for Software Technology

[1] Copyright

Copyright is a form of intellectual property that gives the creator of a work of art or literature, or a work that conveys information or ideas, the right to control how that work is used. Although referred to in the singular, U.S. copyright law actually gives creators (or their assignees and licensees) a number of rights over their works, including the right to reproduce, distribute, adapt or perform them.

To qualify for copyright protection, a work must be "fixed in a tangible medium of expression." Almost any form of expression will qualify as a tangible medium, including a floppy disk, random access memory, printed paper, oil painting or a recording of a radio broadcast.

Copyright shelters only the expression of creativity, not the ideas upon which the expression is based. Copyright may protect a Web page with a "one click" purchase option shown on the page, but it will not protect the idea of one-click purchases. Patent and trade secret intellectual property rights are used to protect the idea upon which the expression is based.

As copyright addresses the expression of the creative work, it has usually been applied to protecting the source code or the user interface of particular software products. Unfortunately, it is fairly straightforward for experienced software designers to develop software that does not infringe a copyright in either the appearance or the source code of another software product. As such, inventors of significantly novel and unobvious

software products prefer to use the more robust protection of patents, which are able to protect not only the program as a whole, but the underlying concepts as well.

[2] Trademark

Patents allow those who create inventions to keep others from making commercial use of the inventions without the creator's permission. Trademark law, on the other hand, is not concerned with how a new technology is used. Rather, it applies to the names, logos and other devices that are used to identify the source of goods or services and distinguish them from their competition.

Patents and trademarks generally do not overlap. However, in the online world where the identity of the source of goods may be the main way to access a patented software product (e.g., the domain name for a Web site), then a trademark may play a valuable role as a nexus to target for preventing or at least delaying infringing activities. If, as is often the case, the patent holder also has a registered trademark that is substantially the same as the infringing domain name, they may be able to take legal action against the infringing domain name or Web site, to prevent or at least frustrate any infringing activities. A likely scenario would be to use the trademark action to shut down or even transfer the domain name in which a patent infringer hosted a Web site with infringing patent material. Of course, seizing a domain name may only delay patent infringing activity until the infringer finds a new domain to host their infringing activity, but at the fast pace of the Internet, a delay is sometimes all that is needed to recapture the market.

[3] Trade Secret

Unlike copyright, federal trademarks and patents, trade secrets are state-based intellectual property rights. A trade secret generally is any formula, pattern, device, idea, process, compilation or information that both: provides the owner of the information with a competitive advantage in the marketplace, and is treated in a way that can reasonably be expected to prevent unauthorized persons from learning about it.

Trade secrets do not require any type of application or registration; one simply must keep the information confidential. Trade secret protection lasts for as long as the secret is kept a secret. Once a trade secret is made available to the public, trade secret protection ends.

Given that trade secrets are protected only so long as they are secret, there is a serious limitation on their utility: any person who discovers the secret independently, without using illegal means or violating agreements or laws is not bound by the trade secret. That means that if someone analyzes or reverse engineers any lawfully obtained product and determines its trade secret, they are no longer bound by that trade secret protection. Further, if they then reveal that information to the public, then all trade secret protection may cease for that trade secret.

In one particularly well known example, a section of source code was posted anonymously to a USENET News discussion group which allegedly was a reverse-engineered version of RSA Security Inc.'s trade secret protected RC4 encryption algorithm.[1] Subsequent testing by readers of the group showed that the code did indeed provide the same output from the same input as the actual RC4 algorithm. The

[1] Loring Wirbel, *RSA Seeks Culprit in Internet Code Posting*, Electronic Engineering Times, September 26, 1994, at 10.

encryption software design community now uses the published source code in place of the RC4 algorithm in products that require RC4 functionality.[2] In an interesting nod to another form of intellectual property protection, the software community refers to the published source code as ARC4 (which stands for "Alleged RC4") as RSA Security still has a trademark on "RC4."[3]

[B] Current Patent Claim Formats for Protection of Software Inventions

The statutory framework established by the Patent Act of 1952, 35 U.S.C. § 101 *et seq*., sets forth with clarity the four main categories of subject matter for which patent protection can be obtained. In particular, 35 U.S.C. § 101 states:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Computer software inventions in general, and Internet-based software applications in particular, lend themselves well to patent claiming techniques covered by three of the four statutory classes. Software inventions have typically been protected by patent claims directed to processes and machines. Two recent decisions by the Court of Appeals for the Federal Circuit ("Federal Circuit"), *In re Lowry*, 32 F.3d 1579 (Fed. Cir. 1994) and *In re Beauregard*, 53 F.3d 1583 (Fed. Cir. 1995), have opened the door to patent protection for software inventions as "articles of manufacture." In response to its acceptance of the decision in *Beauregard*, the U.S. Patent and Trademark Office ("Patent Office") promulgated a comprehensive set of examination guidelines (the "Examination

---

[2] *The Thompson Partnership -- Steganos for Windows 95 - Completely Hide Your Data*, M2 Presswire, December 22, 1997.

[3] *Id*.

Guidelines") for use by patent examiners.[4] In addition, the Patent Office also issued training materials to provide guidance to patent examiners on how best to follow the new examination guidelines. The training materials include a number of patent claim formats that may now be used to protect software inventions.

Four different types of patent claim formats have been used to protect software inventions. Specifically, software inventions have been protected using process claims, apparatus claims, system claims, and stored data structure claims. Apparatus and system claims may recite explicit structural elements, or recite "means plus function" elements. The stored data structure claim format is based on the format approved by the Federal Circuit in *Lowry*, and provides patent protection for novel data structures which "impose a physical organization on the data" stored in a computer memory.[5] In addition, the Federal Circuit's holding in *Beauregard* and the training materials prepared by the Patent Office in response to this case, now permit software inventions to be protected using article of manufacture claims, computer program product claims, and computer data signal claims. Stored data structure claims, computer program product claims, and computer data signal claims are variants of the article of manufacture claim, and as such are deemed patentable by virtue of being stored or embodied in a tangible medium such as a computer memory or carrier wave. Computer data signal claims are referred to as "propagated signal claims," and will be discussed in greater detail in §1.04[A].

---

[4] *Examination Guidelines For Computer-Related Inventions*, 61 Fed. Reg. 7478 (Feb. 28, 1996). The *Examination Guidelines* have been codified in Chapter 2100 of the Manual of Patent Examining Procedure (6th ed., 2d. rev., July 1996).

[5] *In re Lowry*, 32 F.3d 1579 (Fed. Cir. 1994).

In addition to the claim formats described above, the product-by-process claim holds promise as an alternative patent claim format that may be used to provide patent protection for software inventions. This claim format has traditionally been used in the chemical and biotechnological art fields, but may now offer a form of protection for software inventions in view of the revised scope of protection afforded software inventions in *Lowry*, *Beauregard*, and the Patent Office's Examination Guidelines. The product-by-process claim format and its role in providing patent protection for software inventions will be explored in greater depth in §1.04[B].

§ 1.03 LIMITATION OF CURRENT CLAIM FORMATS FOR PROTECTING EMERGING SOFTWARE BUSINESS MODELS

Current apparatus, system, method and computer storage medium claims have developed along with a standard bricks-and-mortar software business model. However, there are a number of new business models that may benefit from the broader scope that emerging claim formats provide.

[A] Downloadable Software Store

As some bricks-and-mortar software stores have gone online to sell their products, some have taken the next step and are delivering the purchased software over the network as well. Egghead used to be a chain of bricks-and-mortar software retail stores, but in 1997 it closed many of its stores and by 1999 had moved all its retail activity to its online site Egghead.com. Although much of what Egghead.com sells is still physically delivered to a purchaser, a portion of the Web site allows customers to download the software they purchase.

Under a conventional analysis, the act of providing a downloadable piece of software which was patented with only conventional apparatus, system, method and computer storage claims may be an infringing activity if the store that provides the downloadable software is in the United States, however, it is not at all clear that if the online store's server containing the downloadable software was located outside the territorial region of the U.S. that any infringing activity would be associated with providing a downloadable copy of a software product that had been patented with conventional apparatus, method and computer storage claims.

Under current patent laws,[6] there are a number of circumstances under which importing or exporting software may be an infringing activity.[7] However, none of the current laws used in conjunction with conventional claim formats indicate that the online store is engaged in infringing activity. The customer would presumably have an infringing copy of the software if they downloaded it, but it would appear that the online store would have imported the software without incurring any liability. This appears to be an unfair outcome. If the online store had shipped a CD-ROM to the customer from outside the jurisdiction of the U.S., they would be liable under 35 U.S.C. § 271(a) for importing a patented product into the U.S. (assuming there was an enforceable computer storage claim that would cover the CD-ROM). However, by accomplishing the same result by downloading the software to a customer connected to a computer network, they are able to escape liability.

---

[6] 35 U.S.C. § 101 *et seq*.

[7] 35 U.S.C. §§ 271(f) and (g).

[B] Application Service Providers

Similar to a downloadable software store, the Application Service Provider ("ASP") business model has emerged in response to the high cost of building custom in-house software solutions. These APSs target businesses that need these types of custom solutions, but are unwilling to bring them in house. An ASP will deploy, host and manage access to packaged applications from a central facility. The applications are then delivered over networks on a subscription basis.

The same unjust results noted above would arise if an overseas ASP provides patented software to a customer in the U.S. if the software was send over a network to the customer business. If the ASP was located in the U.S., they would most likely infringe method, apparatus, system and computer storage claims of any patented custom software they build for the customer business, however simply by locating the ASP overseas (both the servers and the personnel) they would be able to escape liability if they only allow network delivery of their customized software.

[C] Distributed Computing Environments

A number of new forms of software models utilize distributed computing technology such that any one computer program may have its components executing simultaneously on multiple computers, including computers in foreign jurisdictions.

Common Object Request Broker Architecture ("CORBA") is a form of distributed object programming over a network. CORBA allows programs at different locations and developed by different vendors to communicate in a network through an "interface broker."

Distributed Component Object Model ("DCOM") is a set of Microsoft concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network.

Java Remote Method Invocation ("Java RMI") is Sun Microsystems' version of a distributed computing system.

Both DCOM and Java RMI are generally equivalent to CORBA in terms of providing a set of distributed services and they both raise the same issues as CORBA with regard to patented software components or combinations within the distributed network. Accordingly, the authors will use CORBA as an example of a distributed computing environment.

The essential concept in CORBA is the Object Request Broker ("ORB"). An ORB supports a network of clients and servers on different computers. A client program (which may itself be an object attached to an ORB) can request services from a server program or object without having to understand where the server is in a distributed network or what the interface to the server program looks like.

As the client does not know where the server is, a number of interesting problems arise when a client or server unwittingly imports patented software from an ORB or server outside the U.S. First, unlike the ASP or online store, it is not clear who is responsible for the importation of a component in a CORBA enabled network. Each client will only know of its designated ORB, which will then determine which servers should be connected to the client to enable the functionality requested by the client. As some servers on the client's ORB may themselves be clients of other ORBs, the web of

distribution grows at an exponential rate such that running any one client might suddenly cause a chain of connections such that patented software would be imported into the U.S.

The Object Management Group (OMG), which is responsible for the formal specifications defining CORBA has included a licensing service specification in the CORBA design, such that a certain amount of control can be exercised when dealing with intellectual property.[8] Due to the complexity of the interrelations of distributed software objects in the CORBA system, the authors believe that at present, CORBA's internal licensing service is probably the most useful tool for developing a controlled intellectual property protection system for CORBA software components. To the extent that CORBA involves downloading software from foreign servers, it is analogous to the online software store above.

[D] Importation Generally

The Internet is a global network, but data coming from a computer outside a particular country to a computer inside the country is still an importation into that country. The authors are not going to address the potentially relevant, but extremely complex issue of how to determine at what point the importation or copying of software or software products is complete. This particular issue was exhaustively and impressively addressed in an earlier paper by Keith Witek.[9]

The common thread on all the above examples is that although the patented software is imported into the U.S., there is apparently no infringement because under

---

[8] Licensing Service Specification available at:
http://www.omg.org/technology/documents/formal/licensing_service.htm

[9] Keith E. Witek, *Software Patent Infringement on the Internet and on Modem Computer Systems -- Who is Liable for Damages*, 14 Computer & High Tech. L.J. 303, 334-366 (1998).

conventional software patent claims no claimed invention has been imported. The conventional claim formats do not cover the importation of the intangible information that would be in the form of a downloaded software component or program. However, as will be discussed in the next section (§ 1.04), there are emerging claim formats that can be applied to the examples to show direct infringement of the patent claims. Even 35 U.S.C. § 271(g) which prohibits the importation of a product produced by a patented method, would in most cases be insufficient to cover a software component or data structure produced in a foreign jurisdiction by a process patented in the U.S., because the software component or data structure would not be "goods" using conventional claim formats.[10]

§ 1.04 EMERGING PATENT CLAIM FORMATS FOR PROTECTION OF SOFTWARE INVENTIONS

The rapid emergence of the Internet has led to a corresponding increase in the number and variety of commercially important software inventions developed for use on or with the Internet. As technological developments have occurred, so have alternative ways of claiming such developments. The evolutionary development of new patent claim formats has and will most certainly continue to enable patent owners to derive significant financial returns from their investments in patents, especially those directed to the protection of software inventions. As mentioned earlier, recent decisions by the Federal Circuit, and the Patent Office's response to these decisions, have resulted in the creation of several new patent claim formats that will enable patent owners to derive even greater value from patents that protect software inventions.

---

[10] Charles B. Lobsenz and James G. Gatto, *Internet Software May Be Protected Abroad*, 22 Nat. L. J. 8

Two particular patent claim formats now seem to have been accorded a degree of acceptance by the Patent Office that makes them ideal candidates for use in protecting novel software inventions and innovations. These patent claim formats are (1) the propagated signal claim, and (2) the product-by-process claim.

[A] Propagated Signal Claims

[1] Format

The propagated signal patent claim format is directed to a manufactured transient phenomenon, such as an electrical, optical, or acoustical signal, that is embodied in a carrier wave.[11] In order to pass muster, any attempt to use this patent claim format must be directed to a signal that is (1) a manufactured phenomenon, not a natural phenomenon, (2) directed to functional descriptive material embedded in a carrier wave or some other computer-readable medium, rather than functional descriptive material *per se* or non-functional descriptive material, and (3) covered by a specific machine or manufacture, or relates to a practical application in the technological arts.

Computer programs and data structures which are not embedded in some form of computer-readable medium are considered functional descriptive material *per se*. Music, literary works, and pure data are considered non-functional descriptive material since such material cannot be used to cause a computer to perform a particular function. Floppy disks, random access memories, read-only memories, computer hard disks, magnetic tapes, and modulating carrier waves are among the various types of computer-

---

(1999).

[11] Jeffrey R. Kuester, Scott A. Horstemeyer & Daniel J. Santos, *A New Frontier In Patents: Patent Claims To Propagated Signals*, 17 J. Marshall J. Computer & Info. L. 75 (1998).

readable media that functional descriptive material may be embedded in to qualify for patent protection. In most circumstances, a propagated signal will relate to a practical application in the technological arts, and any claim directed to a propagated signal should recite a practical application within a claim limitation. The recitation of the application should not overly limit the scope of the claim as long as it is recited broadly.

Critical to the long-term viability of the propagated signal claim format will be the degree of acceptance it receives from the Patent Office. Although several different types of computer-readable media were identified earlier, the full scope of what constitutes a computer-readable medium has not been fully or clearly articulated by the Patent Office at this time. A broad interpretation of the term "computer readable-medium" will be essential for the long-term economic strength of this claim format. One promising sign was provided in a recent article by the Solicitor of the U.S. Patent and Trademark Office, Nancy J. Linck, who stated that "the PTO is expected to interpret 'computer-readable medium' broadly, perhaps to include a carrier wave for a data signal."[12] The claim format she describes in her law journal article is drawn from the training materials prepared by the Patent Office for patent examiners.

According to the training materials cited by the Solicitor, the general format of a propagated signal claim is as follows:

> A computer data signal embodied in a carrier wave comprising:
>
> (a) a compression source code segment comprising…[recites self-documenting source code]; and
>
> (b) an encryption source code segment comprising…[recited self-documenting source code].

---

[12] Nancy J. Linck & Karen A. Buchanan, *Patent Protection For Computer-Related Inventions: The Past, the Present, and the Future*, 18 Hastings Comm. & Ent. L.J. 659 (1996).

Two patents have been identified, each of which includes a propagated signal claim for the protection of novel aspects of inventions in the data transmission and data communication art fields. The first patent, U.S. Patent No. 5,850,449, was granted to Sun Microsystems on December 15, 1998, and is entitled "Secure Network Protocol System and Method." The abstract for this patent states the following:

> A computer network having first and second network entities. The first network entity includes a packet object generator that generates a packet object including an executable source method, an executable destination method, and data associated with each of the methods. The first network entity also includes a communications interface to transmit the packet object. The second network entity includes a communications interface to receive the packet object and an incoming packet object handler to handle the received packet object. The incoming packet object handler includes a source and destination verifier to execute the source and destination methods with their associated data so as to verify the source and destination of the received object packet.

Claim 20 of this patent includes the following propagated signal claim:

> A computer data signal embodied in a carrier wave, comprising:
>
> instructions for receiving objects transmitted by network entities, wherein at least a subset of the received objects each include source and destination methods and data associated with the source and destination methods; and
>
> an incoming object handler to handle the subset of the received objects, the incoming object handler including a source and destination verifier to execute the source and destination methods of each received object with their associated data so as to verify the source and destination of the received object.

The approach adopted in this claim represents the more conservative model which strictly adheres to the template proposed by the Patent Office in its training materials. This is considered the more conservative approach by the author since this claim *explicitly* recites a propagated signal in a computer-readable medium (i.e., the carrier wave). No cases have yet to be decided which definitively state whether the format of this type of claim necessarily requires the recitation of a computer-readable medium. This approach is consistent with that suggested by the Federal Circuit in *Beauregard*. In the near-term, this is probably the safest form to adopt during the prosecution of an

application before the Patent Office. However, this approach to this type of patent claim suggests that there should be strict adherence to form over substance, which would clearly be contrary to the spirit, if not the letter, of the applicable law. Indeed, there are times when a computer-readable medium may not be present, such as with a purely digital signal comprised of a stream of bits being transmitted in a digital format without being modulated onto an analog carrier wave.[13] Whether a carrier wave must be recited in a propagated signal claim to make it allowable and valid remains uncertain at this time.[14]

A propagated signal claim format which does not explicitly recite a computer-readable medium such as a carrier wave is presented in the second patent, U.S. Patent No. 5,991,330, granted on November 23, 1999, to Telefonaktiebolaget L. M. Ericsson. This patent is entitled "Mobile Station Synchronization Within a Spread Spectrum Communication Systems." The abstract of the patent is provided below:

> Each frame of a pilot channel transmission in a spread spectrum communications system is divided into a plurality of synchronization slots. Each of the synchronization slots includes a pilot code, and at least one of the synchronization slots further includes a framing synchronization code. To extract frame and slot synchronization information from the pilot channel transmission, pilot code timing is first identified by applying a matched filter or correlation to a received pilot signal, identifying peaks, and using the peaks to find a timing reference indicative of synchronization slot boundaries. Next, the set of known framing synchronization codes are correlated with the received signal over the included found synchronization slots. Given that the location within the frame of the known framing synchronization code(s) is known, once a correlation match is found at a certain slot location, the boundary of the frame (i.e., the frame synchronization) relative thereto is then also known.

A propagated signal claim is included in Claim 1 and it states the following:

> A propagated signal for a code division multiple access pilot channel transmission, comprising:
> a repeating frame comprising a plurality of synchronization slots;
> a pilot code c_p repeated in each synchronization slot of the repeating frame; and

---

[13] Kuester, Horstemeyer & Santos, *supra* note 3, at 86.
[14] *Id.*

> a framing synchronization code c_s in at least one of the synchronization slots of the repeating frame.

This second example of a propagated signal claim is representative of a claiming strategy which does not explicitly identify the computer-readable medium in which the propagated signal is embodied. The patent was filed the year after the codification of the Examination Guidelines in the *Manual of Patent Examining Procedures*, and the publication and distribution of the related training materials to the Patent Office's corps of patent examiners. The mere fact that this claim was allowed by the Patent Office suggests that it may not be necessary to explicitly recite a computer-readable medium in a propagated signal claim. However, this is contrary to the requirement set forth in the Examination Guidelines, which indicate that this type of claim will only be statutory if it is directed to functional descriptive material embodied in a computer-readable medium having a practical application in the technological arts.

[2] Strategic Advantages

The propagated signal claim format arguably provides three strategic advantages. First, it may allow patent applicants to significantly reduce the total cost of obtaining patent protection by obviating the necessity for separate sets of independent claims directed to signal transmitters and signal receivers. The mere transmission of a propagated signal would be sufficient to impose liability on the transmitting party regardless of whether such party is using the appropriate transmitter or receiver. Notwithstanding this apparent advantage, separate sets of claims directed to signal transmitters and receivers should continue to be included until the Federal Circuit definitively declares that propagated signal claims constitute statutory subject matter.

The second major advantage provided by propagated signal claims is the significantly increased breadth of coverage. No longer will it be necessary for a patent owner to determine whether an alleged infringer is transmitting a propagated signal using an infringing transmitter or an infringing receiver. Instead, all that a patent owner would need to establish would be the mere fact of transmission of the propagated signal over some form of computer-readable medium, such as electrical wires, optical fiber, free-space optical channels, or water. Indeed, this type of claim may hold considerable promise for the owners of patents on the myriad of signals to be propagated in the upcoming era of mobile electronic commerce, commonly referred to as "mCommerce." Among the range of mCommerce applications to be developed which may by protected by one or more propagated signal claims will be those involving the Bluetooth standard (see http://www.bluetooth.com/), as well as computationally powerful applications involving human-implantable wireless devices, remote diagnosis and repair of consumer and industrial appliances, and voice activated Web sites embedded with automatic speech recognition and translation capabilities.

The third strategic advantage provided by propagated signal claims will be their relative ease of discovery. In many cases, it will be possible to capture a signal and analyze it directly to establish infringement without the need to know how a transmitter or receiver uses the infringing signal. Analysis may be performed using a computer, an oscilloscope, or a spectrum analyzer. A logic analyzer, a protocol analyzer, or a deep memory oscilloscope may also be used in the analysis of patented propagated signals. One potentially challenging aspect of this apparent advantage will be determining how best to sift through the great number of signals likely to be propagated between

application providers who generate these signals, access providers who will be responsible for aggregating and transmitting the signals, and end-users in possession of signal receivers, whether stationary or mobile, who will more than likely be bombarded by multitudes of propagated signals. These are problems industry will have to address soon to avoid a super-exponential increase in patent infringement suits.

[B] Product-By-Process Claims

[1] Format

A product-by-process claim defines a product at least in part in terms of the method or process by which it is made.[15] In the past, the traditional rule in the Patent Office was a 'rule of necessity' and permitted a claim to a product to be defined by reference to the method of its production only when the product could not be adequately defined in any other fashion. The current rule in the Patent Office places a greater emphasis on satisfying the definiteness requirement.[16] Specifically, product-by-process claims will be allowable, even if the invention can be described in purely structural terms, as long as the definiteness requirement is satisfied (i.e., the claim must particularly point out and distinctly claim the invention). The resulting product must still be novel in structural terms and must in any event satisfy the nonobviousness requirement. The court in *In re Pilkington*, 411 F.2d 1345, 162 U.S.P.Q. 145 (C.C.P.A. 1969), stated the patentability requirement for a product protected by a product-by-process best when it concluded that, "patentability of a claim to a product does not rest merely on a difference

---

[15] Donald Chisum, 3 *Chisum On Patents*, § 8.05 (1991)(citing *Bonito Boats, Inc. v. Thunder Craft Boats, Inc*., 489 U.S. 141, 9 U.S.P.Q.2d 1847, 1855 (1989)).
[16] *Id*.

in the method by which that product is made. Rather, it is the product itself which must be new and unobvious."[17]

Product-by-process claims are not specifically discussed in the patent statute. Instead, these types of claims are creations of the courts, which they felt compelled to develop in those instances when the definition of a product in terms of strict structural limitations was impossible or extremely difficult. For this very reason, even though product-by-process claims are limited by and defined by the process used to make the resulting product, the determination of patentability in the Patent Office is based on the product itself.[18] The Patent Office's treatment of product-by-process claims as a product claim for patentability is deemed consistent with policies giving claims their broadest reasonable interpretation.[19]

Notwithstanding their treatment in patentability determinations before the Patent Office, the same rule does not apply to product-by-process claims in validity and infringement disputes in courts. Process terms in product-by-process claims serve as limitations in determining infringement.[20] This is consistent with Supreme Court precedent which was stated unequivocally in an early product-by-process patent dispute that "nothing can be held to infringe the patent which is not made by that process."[21] Product-by-process claims will be interpreted the same in court proceedings whether for

---

17 *In re Pilkington*, 411 F.2d at 1348.

18 *Atlantic Thermoplastics Co., Inc. v. Faytex Corp.*, 970 F.2d 834, 23 U.S.P.Q. 2d 1481 (Fed. Cir. 1992).

19 *Id*. at 846.

20 *Atlantic Thermoplastics*, 970 F.2d at 846-47.

21 *Atlantic Thermoplastics*, 970 F.2d at 842 (citing *General Electric v. Wabash Appliance*, 304 U.S. 364, 373-74, 82 L.Ed. 1402, 58 S. Ct. 899 (1938)).

validity or infringement purposes.[22] Since process terms limit the scope of product-by-process claims in the infringement and validity context, and thus tend to prevent them from being read as broadly as product claims including only structural limitations, the Federal Circuit has stated that "an applicant could claim a product in product-by-process terms as a hedge against the possibility that those broader product claims might be invalidated."[23]

Claiming a product using a product-by-process claim format does involve a price. Specifically, the Court of Customs and Patent Appeals stated in an early decision that in the case of product-by-process claims,

> the Patent Office is not equipped to manufacture products by the myriad of processes put before it and then obtain prior art products and make physical comparisons therewith… [T]he Patent Office bears a lesser burden of proof in making out a case of prima facie obviousness for product-by-process claims because of their peculiar nature than would be the case when a product is claimed in the more conventional fashion.[24]

In view of the foregoing, it appears that the following must be provided if a claim is to be construed as defining a product-by-process:

1. The claim must be directed to a product.
2. The claim must include limitations that are procedural and not structural.
3. The process limitations must describe the making of the product, not how the product is used.
4. The process limitations must be significant to the definition or description of the product.[25]

However, it should be remembered that such claims are subject to a lesser burden of proof on the issues of novelty (35 U.S.C. § 102) and obviousness (35 U.S.C. § 103),

---

[22] *Atlantic Thermoplastics,* 970 F.2d at 846.

[23] *Atlantic Thermoplastics*, 970 F.2d at 844.

[24] *In re Fessmann*, 489 F.2d 742, 180 U.S.P.Q. 324, 325-26 (C.C.P.A. 1974).

and thus may be more susceptible to challenges based on these issues than conventional product claims.

Product-by-process claims may be written as either independent or dependent claims. There are two general forms of product-by-process claims. The first form is a *pure* product-by-process claim and it defines the claimed product only by the process that produces the product. The following is representative of this form of a product-by-process claim:

> An article of manufacture prepared by a process comprising:
> step A;
> step B; and
> step C.[26]

In the software context, an article of manufacture may include a data structure, a computer program product or a propagated signal. One practical example of a pure product-by-process claim which was the subject of the dispute in the *Atlantic Thermoplastics* case was the following:

> The molded innersole produced by the method of claim 1.

An additional practical example of a pure product-by-process claim is below:

> The coffee extract obtained by the process defined in claim 6.

The second form of the product-by-process claim involves a combination of structural and process limitations. An example representative of this approach is shown below:

> A resistor which comprises:
> (a) a ceramic core;
> (b) a coating of carbon deposited on the core by decomposition of a hydrocarbon gas in the presence of the core; and

---

[25] Irah H. Donner, *Patent Prosecution: Practice & Procedure Before the U.S. Patent Office*, 2d. ed., 588 (1999).

[26] *Id*. at 589, footnote 373, *citing* 2 Irving Kayton, *Patent Practice* 5:10-43 (4th ed. 1989).

(c) a stripe of conducive metal….etc.

(or, (b):…by decomposing a hydrocarbon gas in the presence of the core…)[27]

The primary issue with these types of product-by-process claims is how best to determine the process limitations that will convert an article or product claim into a product-by-process claim. This example was relatively clear. In general, however, no clear guidance has been provided by the Federal Circuit on what type of process limitation will result in the conversion of a product claim having at least one process limitation into a product-by-process claim.[28] This is currently an unsettled area of the law and applicants should be careful to craft product claims using only structural limitations if the intent is to have such claims examined as products. Alternatively, applicants should include only process limitations in claims used to make products that would be difficult, if not, impossible to describe using only structural limitations if the intent is to have these types of claims examined by the Patent Office as product-by-process claims.

[2] Strategic Advantages

The product-by-process claim format arguably provides at least three different strategic advantages. First, this claim format can be used as a secondary or 'fallback' position during the patentability determination phase before the Patent Office. As Circuit Judge Rader stated in *Atlantic Thermoplastics*, "an applicant could claim a product in product-by-process terms as a hedge against the possibility that those broader product

---

[27] Robert C. Faber, *Landis On Mechanics of Patent Claim Drafting*, § 46 (4th ed. 1999).

[28] The Federal Circuit has even acknowledged this fact in one case in which it stated that "[simply because] a process limitation appears in a claim does not convert it to a product by process claim." *Fromson v. Advance Offset Plate, Inc.*, 720 F.2d 1565, 219 U.S.P.Q. 1137, 1141 (Fed. Cir. 1983).

claims might be invalidated."[29] Thus, product-by-process claims, while not enjoying the breadth of claim coverage provided by product claims including only structural limitations, do provide some additional protective ammunition in the contest for patent protection in any patentability determination before the Patent Office.

A second advantage provided by product-by-process claims is the claim drafting flexibility provided to patent applicants. In those instances when it is very difficult, if not impossible, to readily define the structural scope of a product claim, product-by-process claims may be used to claim a product exclusively in terms of process limitations. As mentioned earlier, such claims may also be a combination of procedural and structural limitations; however, there is no bar to using only procedural limitations in product-by-process claims. This additional flexibility in claim drafting strategy may be extremely beneficial in these instances.

The third and perhaps most significant advantage provided by product-by-process claims is their use as barriers to prevent the importation of novel and nonobvious products which nevertheless defy any attempt to define them strictly in terms of structural limitations. Product-by-process claims are a form of article of manufacture claim and as such apply to novel computer program products, data structures, and propagated signals. Use of this claim format would be appropriate where such articles of manufacture are not embodied in a computer-readable medium, *per se*, or are not readily capable of definition using structural limitations exclusively.

Based on what guidance has been provided by court decisions in this field, a computer program product that is not embedded in a computer-readable medium but

---

[29] *Atlantic Thermoplastics*, 970 F.2d at 844.

which is produced by a novel computer-implemented algorithm which imparts some novel structure on the product may qualify for patent protection using a product-by-process claim. The patentability determination will consider only the novelty and nonobviousness of the computer program product. In an infringement or validity dispute, however, a court would consider the novelty and nonobviousness of the automated process applied by the computer-implemented algorithm as well as the novelty and nonobviousness of the resulting computer program product when evaluating the product-by-process claim.

In addition, if a separate product-by-process claim is drafted which defines a propagated signal containing data for this program, then the process of generating the signal as well as the structure of the signal itself would also be evaluated in an infringement or validity litigation. This may be a particularly challenging evaluation for a court if the structure of the signal cannot be readily gleaned from the procedural limitations in the applicable product-by-process claim. The structure of the signal alone would be considered in a patentability determination of the claim before the Patent Office. Hence, a product-by-process claim could potentially be a very useful and effective tool available to a patent owner seeking relief from extra-territorial activity involving the generation and importation by signal transmission of a protected signal or a protected computer program product which may have a significant economic affect in the United States.

§ 1.05 ENFORCEMENT ISSUES

[A] Legal Enforcement

The emerging claim formats will make little or no difference in the enforcement of legal remedies if conventional claim formats are also infringed. Accordingly, the discussion will be limited to scenarios in which it is unlikely that a conventional claim would cover the infringing activity.

[1] Best Case Scenario

In a best case scenario a remote Web site on a server outside the U.S. is sending infringing software into the U.S., however, the owner of the server and the Web site is the same person and it is located in the U.S. within reach of a court of competent jurisdiction.

[a] Jurisdiction

The good news about obtaining personal jurisdiction is that for patent infringement cases, after interpreting the state's long arm statute, jurisdiction is determined under the Federal Circuit's three prong *Akro*[30] test in which the full extent of due process is used to interpret if there is personal jurisdiction. In a best case scenario this would include an infringer that was located in or specifically targeted their infringing activity at the state in which a suit is brought.

[b] Traceable Pattern of Infringement

In addition to having jurisdiction, a best case scenario would have a clear and traceable pattern of infringing activity. As mentioned earlier, propagated signal claims often make it easier to determine if infringing activity is taking place. In a best case

scenario, and readily identifiable propagated signal could be easily intercepted to provide a statistically significant indication of the amount of infringing activity.

[c] Deep Pockets

Finally, for any legal remedy to be considered successful, the infringer must have sufficient assets within the court's jurisdiction to cover the cost of any remedies at law the court may determine.

[2] Worst Case Scenario

In a worst case scenario a remote Web site on a server outside the U.S. is sending infringing software into the U.S. However, the owner of the server and the Web site are two different unidentified people and they are both known to be located outside the U.S. in a country which does not recognize decisions or judgments by U.S. courts. Furthermore, they would both have no assets within reach of any court of competent jurisdiction.

[a] Jurisdiction

A recent article in *Wired* magazine provides an ideal example of a worst case scenario for jurisdiction purposes.[31] Sealand is a World War II gun platform that has been turned into an independent nation. Sealand's only commercial enterprise and the occupier of all of its real estate is a company called Havenco. Havenco's express purpose

---

[30] *3D Systems, Inc. v. Aarotechlaboratories, Inc., Aaroflex, Inc., and Albert C. Young*, 160 F.3d 1373, 1377; 48 U.S.P.Q.2d (BNA) 1773 (Fed. Cir. 1998) citing *Akro Corp. v. Luker*, .45 F.3d 1541, 1544; 33 U.S.P.Q.2d (BNA) 1505, 1507 (Fed Cir. 1995).

[31] Simson Garfinkel, *Welcome to Sealand. Now Bugger off.*, Wired, July 2000, p. 230.

is to "give people a safe, secure shelter from lawyers, government snoops, and assorted busybodies.[32]"

Accordingly, assume that the server and the Web site are located in Sealand, and that the owners of the server and the Web site have both taken advantage of Havenco's ability to host information and Web sites anonymously,[33] and that all payments for the infringing software are in some type of anonymous bearer instrument such as cash or precious metals that are sent to a jurisdiction who will not honor a subpoena from a U.S. court.

[b] Untraceable Pattern of Infringement

Another hurdle that would be likely in our Sealand scenario is that any propagated signal from the server is likely to be over an encrypted channel. Therefore, even though it is possible to determine that information is being sent from the server, it would not be possible to match the signal with a pattern of bits that may indicate that the propagated signal contains the patented software. Encrypted signals have reached sufficient sophistication that it is for all intents and purposes impossible to determine their contents, even with the most sophisticated computing resources on the planet,[34] especially considering that the information merely has to be protected for approximately the length of the remaining patent term.

---

[32] *Id*.

[33] http://www.havenco.com/about_havenco/faq.html, FAQ #3.

[34] Matt Blaze et al., *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*, available at http://www.counterpane.com/keylength.html, distributed January 1996.

[c] Judgment Proof

Finally, to add insult to injury, if the anonymous infringers have no identifiable assets, then any remedy at law would be moot.

[B] Equitable Enforcement

Of substantial interest, given that remedies at law may not be possible in many circumstances, is the possibility of equitable enforcement. Although it may be of more interest, it is not necessarily an approach that is any more likely to bring success.

[1] Enforcing Injunctive Remedies

Enforcing equitable remedies on the Internet is extremely difficult when an infringer has planned to use technology and the law to shield themselves. One of the early pioneers on the Internet, John Gilmore, summed up the issue quite well: "The Net interprets censorship as damage and routes around it.[35]" The Internet has a long tradition of resisting any encroachment on disseminating information, even illegal, unpopular or infringing information. As the Internet is a global system, there have been a number of prominent cases where people have gone "forum shopping" to locate a place where their information could be disseminated freely. Although the examples below are not of patent infringers, their technological and legal responses in attempts to curtail their activities are applicable to a patent infringer seeking to limit any technological or equitable enforcement action.

Instead of examining the incidents of technological responses and forum shopping directly, each example presupposes that a court has approved an equitable or

---

[35] *SPECIAL REPORT: Redefining Community -- Technology Gives Us Enormous Leverage - But We Must Learn To Use It*, InformationWeek, November 29, 1993, at 28.

technological remedy. These remedies will then be followed by an actual response to that form of remedy on the Internet.

[a] Domain Name Transfer

One common problem with restricting activities on the Internet is where to find a nexus to attack that will totally stop the infringing activity. As mentioned above, the domain name used to identify an infringing Web site is a particularly attractive target if it is the main source of infringing activity. Assume then that a court has issued an injunction to a domain name registrar to disable a domain name and not reissue it to anyone. Such was the case of VOTEAUCTION.COM.

[i] Responses - VOTEAUCTION.COM

VOTEAUCTION.COM was the brainchild of a college student who supposedly wanted to point out the hypocrisy of corporations paying large quantities of money to other large corporations to sway the votes of individual people.[36] His attempt at satire was to allow individuals to submit their votes for interested parties to bid on the privilege of determining whom the votes should be cast for. Apparently the satire was lost on the Chicago Board of Elections, on October 18, 2000, where an Illinois circuit court issued an injunction seizing the domain name.[37] The site then opened under another name: VOTE-AUCTION.COM (with a hyphen). In an apparent success story for the prosecution, the Internet Council of Registrars (CORE) then voluntarily honored a temporary restraining order issued by the Wisconsin Attorney General to remove the new domain name. However, even though both domain names were out of commission, the

---

[36] Mark K. Anderson, *Close Vote? You Can Bid on It*, Wired News, August 17, 2000.

Internet protocol (IP) address of the site remained (and as of this writing on December 18, 2000 remains) available at http://62.116.31.68.[38]

Unlike the VOTEAUCTION.COM case, it is unlikely that the patent owners will have the level of support that the prosecution was able to garner. Accordingly, although eventually two domain names were withdrawn from use, there was nothing that could be done to remove the IP address, and the Web site still remains accessible.

[b] Site Blocking

Another approach that has been tried is to try to block access to a particular Web site. Assume then that a court has issued an injunction to all Internet Service Providers (ISPs) in the U.S. that they are required to block a particular Web site, even though this may seem a little far fetched. Such was essentially the case when the German Office of Public Prosecution threatened to confiscate ISPs' computers and possibly fine or imprison the personnel of any that did not comply by blocking a link to a Dutch Web Site carrying the text of a leftist magazine called *Radikal*.

[i] Responses - *Radikal* and XS4ALL

The response was swift. The Dutch ISP, XS4ALL, took anti-censorship measures on its own first. It proceeded to rotate the IP address that the Web site mapped to, such that any block by a German ISP would only be temporary until a new IP address was assigned to the Web site.[39] The German prosecutors eventually requested that all of XS4ALL's IP addresses be blocked, even though it meant blocking all the Web sites

---

[37] Brian Krebs and David McGuire, *Vote-Auction.com Back Online; Authorities Ponder Next Move, Newsbytes*, November 2, 2000.

[38] *Id.*

[39] Personal conversation of one of the authors with a participant in the mirroring campaign.

hosted on XS4ALL. This was equally ineffective as a "mirroring" campaign was organized to replicate the *Radikal* Web site to multiple locations, such that Germany would eventually have to shut down all Internet access to prevent access to the Web site.[40] The mirroring campaign achieved its purpose, and none of the individuals involved were convicted of any crimes.[41]

What is significant to keep in mind for purposes of patent infringement, is that mirroring does not have to be an Internet-wide campaign with multiple people involved in a nonviolent protest movement. Rather, it is possible for one scofflaw infringer to set up multiple mirrored Web sites, such that as one is found, the next is activated. Although in many cases, for a small-time infringer, notifying their ISP may be sufficient to stop the infringing activity; if the infringer wants to fight back, and is personally out of reach, attacking a Web site is almost always unsuccessful.

[C] Suing the Providers

Although in theory, the intermediate providers of Internet connectivity between an infringing overseas server and a U.S. based customer may be infringers under a strict liability analysis of current U.S. law,[42] the authors do not believe that this should be the case, given the enormous expense that would then have to be passed on to customers of ISPs potentially liable for patent infringement. In the following section, the authors

---

[40] Jim McClellan, *Cyberlife UK: Germany Calling*, The Guardian, September 26, 1996 at 13 and Martin Bensley, *Germany Chases Radical Newspaper Along Information Superhighway*, Deutsche Presse-Agentur, September 17, 1996.

[41] *German Court Dismisses Criminal Charge Over Internet Use*, Electronic Crimes Enforcement, August 1997, Vol. 13, No. 8.

[42] Keith E. Witek, *Software Patent Infringement on the Internet and on Modem Computer Systems -- Who is Liable for Damages*, 14 Computer & High Tech. L.J. 303, 334-366 (1998).

explore a number of possible regulatory changes to balance the potential liabilities under the current system.

§ 1.06 Potential Regulatory Responses

[A] Potential Parties

A number of parties may become entangled in a variety of intellectual property disputes involving the importation into the United States of patent protected software inventions. Among those parties having the greatest potential exposure to liability for the transmission of signals, whether protected as propagated signals embedded in computer-readable media or as novel products-by-process, will be ISPs and telephone companies. Certainly, ASPs offering content that is transmitted on signals which are imported into the United States will also face a significant risk of liability for patent infringement to the extent the signals they generate and transmit into this country are protected by a patent.

In addition, the manufacturers and sellers of the equipment used to transmit and receive propagated signals will face potential liability for contributory or induced patent infringement. It will be a virtual certainty that the public at large will face the most significant risk from the widespread enforcement of these patent claims since they will most likely be forced to pay the cost of litigation in the form of higher rates for the panoply of services provided by ISPs, telephone companies, and ASPs. Thus, there is the very real possibility that these new claim formats may pose serious threats to the continued development and use of the Internet as a channel for commerce in the future unless legislative action is taken to minimize or eliminate the liability that may result from such litigation risks.

[B] Potential Scope of Liability for Patent Infringement

The potential scope of liability for patent infringement could be staggering for many of the most stalwart Internet businesses, especially at the present time given the rapid growth in the number of wireless devices in communication with Internet information services based here and abroad. Several authors have already written about the potential explosion in patent infringement litigation that may be brought about by the use of these new claim formats. Some have proposed reasonably creative solutions to this problem. However, it is a problem that will definitely grow in complexity and magnitude in the next two to five years unless legislation is enacted that directly addresses this problem.[43]

The patent statute sets forth the standard for direct patent infringement in 35 U.S.C. § 271(a), which states in pertinent part that "whoever without authority makes, uses, offers to sell or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent."[44] This section makes it clear that no level of intent, knowledge, or inducement need be established to prove direct patent infringement. In short, it is a strict liability offense that may subject the parties mentioned earlier to significant risks of liability for patent infringement for the mere transmission of a signal protected by a patent as a propagated signal or a product-by-process.

---

[43] Kuester, Horstemeyer & Santos, *supra* note 3; Lee A. Hollaar, *Justice Douglas Was Right: The Need For Congressional Action On Software Patents*, 24 AIPLA Q.J. 283 (1996); Wilson, *infra* note 50; Raymond Van Dyke, *Software Patents Offer Opportunities And Obstacles: 'State Street' Sparked A Boom In PTO And Court Filings, And the Dust Has Not Quite Settled*, 21 Nat. L. J. 39 (1999); Charles B. Lobsenz & James G. Gatto, *Internet Software May Be Protected Abroad: Counsel's Challenge Is To Overcome Policy, Statutes And Case Law That Limit U.S. Patents' Scope To The Nation's Borders*, 22 Nat. L. J. 8 (1999).

[44] 35 U.S.C. § 271(a).

By contrast, sections 35 U.S.C. § 271(b) and 35 U.S.C. § 271(c) set forth the definitions for induced and contributory patent infringement, respectively. In the case of induced patent infringement, the patent statute states "[w]hoever actively induces infringement of a patent shall be liable as an infringer."[45] The definition of contributory infringement is stated as follows: "[w]hoever offers to sell or sells within the United States or imports into the United States a component of a patented machine, manufacture, combination or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer."[46]

Note well that *active inducement* is the standard set by the statute for liability to attach. In the case of an Internet-based venture, any active marketing or promotion of a service purporting to offer various forms of compelling information or content over the so-called "wireless Web" may very well find itself in an expensive Faustian bargain. As for contributory infringement, the statute makes it clear that knowledge must be proven before liability will attach. Thus, any efforts by ASPs to actively promote the use of their wireless Web services using specialized plug-in software designed to be compatible with the existing base of cellular telephones, personal digital assistants or other related personal information devices may expose them to liability for contributory patent infringement if the plug-ins they distribute are designed to receive or retransmit signals

[45] 35 U.S.C. § 271(b).
[46] 35 U.S.C. § 271(c).

which are protected by patent. Furthermore, if ISPs and telephone companies are aware of the transmission of such signals into the United States, they too will be exposed to the risk of being held liable for contributory patent infringement even when the transmitters used by the ASP are based offshore.

In addition to the risk of liability for direct, induced and contributory infringement, there is also the added risk of liability for direct infringement resulting from the mere importation of a conventional, unprotected software product that is made by a process protected by patent in the United States.[47] This section of the patent statute may be problematic for an Internet ASP that performs data transfers over the Internet which are not modulated onto analog carrier waves, but which are transmitted by novel data communication patterns produced by a process patented in the United States. Direct infringement liability may attach in this case for infringement of a process patent claim or a product-by-process claim.

It should also be noted that 35 U.S.C. § 271(c) bars the importation of a component of a patented machine or manufacture, as well as any material or apparatus to be used to practice a patented process constituting a material part of an invention. Hence, this section may cause ASPs, ISPs, and telephone companies to be liable for the transmission into the United States of signals containing portions of novel structures that may be patented in this country. Arguably, this section of the patent statute could provide a patent owner with the ability to directly affect commercial activity beyond the borders of the United States.

[47] 35 U.S.C. § 271(g).

Two other sections of the patent statute also provide the basis for imposing liability on ISPs, ASPs, and telephone companies engaged in the transmission of data on modulated or unmodulated signals into the United States. These sections of the patent statute are 35 U.S.C. § 271(f)(1) and 35 U.S.C. § 271(f)(2). The first section states "Whoever without authority supplies or causes to be supplied in or from the United States all or a substantial portion of the components of a patented invention, where such components are uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the patent if such combination occurred within the United States, shall be liable as an infringer."[48]

This section may apply to an Internet service in which data is solicited and compiled from numerous sources (e.g., industry specific data compilation), and then combined in a novel way, perhaps on one or more mirrored Web sites on the Internet, and transmitted into the United States in the form of a signal that may be patented in this country as a novel article of manufacture. By promoting such a service, an ASP may be held liable for "actively inducing" end users to contribute data that would be combined, processed and transmitted in a novel propagated signal.

This scenario may sound far-fetched, but imagine a specialized service offered by an automobile manufacturer and service provider which allowed purchasers to enroll in a service that involved the automatic diagnosis and correction of problems in the electrical subsystems of their automobiles. If the manufacturer included microchips in their automobiles that could be activated upon enrollment in such a service, the data could be

[48] 35 U.S.C. § 271(f)(1).

compiled and reported to one or more servers offshore. Afterwards, a master service control signal could be transmitted at predetermined times which automatically diagnosed and repaired such problems in these automobiles. If this master service control signal is sufficiently novel, it may be patented in this country, and any transmission into the country by a third party may constitute an infringement of this patent. In addition to signal transmission, the automatic compilation and storage of data in a novel data structure in the onboard computer memory included in the automobiles may also result in liability for infringement of patent claims directed to the storage of the data structure in a computer-readable medium, such as a memory chip.

The second section listed above imposes liability under a slightly different set of circumstances. It states "Whoever without authority supplies or causes to be supplied in or from the United States any component of a patented invention that is especially made or especially adapted for use in the invention and not a staple article or commodity of commerce suitable for substantial non-infringing use, where such component is uncombined in whole or in part, knowing that such component is so made or adapted and intending that such component will be combined outside of the United States in a manner that would infringe the patent if such combination occurred within the United States, shall be liable as an infringer."[49]

This section of the patent statute places greater emphasis on the supply of components that are "especially made or especially adapted" for use in an invention. It also requires knowledge and intent to be proven before liability will attach for direct infringement. In the event that patent claims directed to propagated signals, and product-

by-process claims directed to software products produced by novel processes, gain wider acceptance and usage, then conceivably there may be greater industry knowledge about which types of signals, or data streams embedded in signals, are used in certain forms of online commerce. If this situation develops, then it may soon become possible to prove that an alleged infringer developed and knowingly supplied one or more components that were specially made with the intent of combining them offshore into a protected software invention which is subsequently transmitted into this country on one or more propagated signals.

It should be clear from the discussion of these relevant sections of the patent statute that liability may be imposed on a number of entities for various forms of patent infringement. Certainly ASPs who transmit signals into the United States which are protected as patented products-by-process or as patented propagated signals will be liable for direct patent infringement. In addition, under a vicarious liability theory, a number of ISPs and telephone companies may also be held liable for patent infringement.[50] The imposition of liability for patent infringement on telephone companies and ISPs would be a profoundly unfair result. However, the patent statute in its current form provides no "innocent infringer" defense and would therefore dramatically increase the exposure these companies would have to the risk of being held liable for patent infringement. Clearly, some form of legislative protection is needed to address the emerging risks these important service providers will soon confront.

---

[49] 35 U.S.C. § 271(f)(2).

[50] Dana M. Wilson, *The Propagated Signal Claim: What Is It and What Are The Infringement Consequences*, 6 J. Intell. Prop. L. 425, 447 (1999).

[C] Proposed Statutory Revisions

It is not presently possible to determine with any degree of reliability how broadly or restrictively courts will construe the scope of the emerging claim formats for software inventions, especially those claim formats which will apply to the importation of propagated signals transmitted from locations beyond the national borders of the United States. Despite this lack of clear guidance from the courts, it may be reasonable to assume that the scope of activity that will likely constitute infringement will be massive and far-reaching. Some form of legislation should be enacted to provide a 'safe harbor' for ISPs and telephone companies since these two groups of companies will in all likelihood have very little, if any, control over the myriad of signals passing through their communication systems.

The statutory provisions limiting the liability of parties for copyright infringement on the Internet, which have been included in the Digital Millennium Copyright Act of 1998 (the "DMCA"),[51] may be helpful in determining how best to establish a workable scheme for limiting the liability of ISPs and telephone companies for 'innocent' patent infringement. The DMCA expressly sets forth four different limitations on liability for online copyright infringement by online service providers. The limitations are based on the following categories of conduct by a service provider: (1) transitory communications, (2) system caching, (3) storage of information on systems or networks at the direction of users, and (4) information location tools.[52] Only the first two liability limitations appear applicable to the situation involving the potential extra-territorial reach of patents

---

[51] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

[52] 17 U.S.C. §§ 512(a) – (d).

covering a signal or a product-by-process and only they will be discussed below. The copyright statute also includes a defense to copyright infringement referred to as 'fair use,' which may also be a viable means for introducing an 'innocent infringer' defense in the patent statute.[53]

The first limitation focuses on limiting the liability of service providers for online copyright infringement involving transitory communications. The copyright statute defines a service provider for the purpose of this first liability limitation as "[a]n entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[54] In this particular case, the limitation is intended to limit a service provider's liability in circumstances where the provider merely acts as a data conduit, transmitting digital information from one point on a network to another at the request of a third party. This limitation applies to the acts of transmitting, routing, or providing connections for the information, as well as the automatic generation of intermediate and transient copies which occur during the operation of a network.[55]

A service provider will qualify for this limitation if the following conditions are satisfied: (1) the transmission, routing, provision of connections, or copying must be carried out by an automatic technical process without selection of material by the service provider; (2) the service provider must not determine the recipient(s) of the material; (3)

---

[53] 17 U.S.C. § 107.

[54] 17 U.S.C. § 512(k)(1)(A).

[55] The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, 10 (Dec. 1998).

any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients, and must not be retained for longer than reasonably necessary; and (4) the material must be transmitted with no modification to its content.[56]

The term 'service provider' is defined somewhat differently for the second applicable liability limitation. In this case, the term is defined as including an entity described in the previous definition, but adds that a service provider will also be "[a] provider of online services or network access, or the operator of facilities therefor…"[57] In general, the second limitation on liability for copyright infringement limits the liability of service providers for the practice of retaining copies, for a limited time, of material that has been made available online by a person other than the provider, and then transmitted to a subscriber upon request. In this scheme, a service provider would retain the material so that subsequent requests for the same material could be fulfilled by transmitting the retained copy, rather than retrieving the material from the original source on the network.[58]

A service provider will qualify for this liability limitation if: (1) the content of the retained material is not modified, (2) the provider complies with applicable rules about 'refreshing' material, (3) the provider does not interfere with technology that returns 'hit' information to the party that posts such material, (4) the provider limits access to the material in accordance with access restrictions imposed by the party that posts the material online, and (5) any material that was posted without the copyright owner's

---

[56] *Id.*

[57] 17 U.S.C. § 512(k)(1)(B).

[58] See *supra* note 31.

authorization is removed or blocked promptly once the service provider is notified that it has been removed, blocked, or ordered to be removed or blocked at the originating site.[59]

The fair use defense to copyright infringement has not yet been precisely defined although it has been used successfully in a number of cases. The copyright statute has codified the four essential factors courts have determined to be important when determining whether the use of a copyrighted work constitutes fair use. These four factors are: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[60] This defense includes factors which are subject to subjective interpretation and is probably not the strongest base upon which a defense to patent infringement on a theory of 'innocent infringement' can be created.

The various liability limitations presented above represent the result of a realistic assessment of the bases of copyright infringement in the new 'digital era.' It is our contention that the same notions of fairness that led to the development of these defenses to copyright infringement, which appear to strike a reasonable economic bargain between the interests of copyright owners and the well-being of the public at large, apply equally in the context of patent infringement. The sheer volume of traffic generated on the Internet today is already straining the existing base of computing resources available to serve the millions of users around the world.

---

[59] See *supra* note 31 at 12.
[60] 17 U.S.C. § 107.

The trend toward the integration of wireless communication capabilities with the computing infrastructure available on the Internet today, along with the rapid advances in hardware design that will lead to an ever-increasing base of computing capability in the near future, strongly suggests that the task of identifying and monitoring individual signal transmissions will overwhelm the abilities of even the most capable online service providers. In this evolving environment, it simply will not be possible to place the undue burden of patent infringement litigation on ISPs and telephone companies that may unknowingly be engaged in the transmission of patent protected signals generated from beyond the national borders of the United States.

By placing a disproportionate burden of the risk of patent infringement litigation on ISPs and telephone companies, the overall cost of providing services on the Internet to consumers will eventually become unacceptably high, and the end result will likely be an unfortunate dissipation of the Internet's true commercial potential. A legislative solution has been developed to provide service providers with 'safe harbors' limiting their liability for copyright infringement. It is now time to adopt comparable safe harbors to limit their liability for 'innocent' patent infringement.

§ 1.07 Conclusion

While a valuable new set of tools has been added to the tool chest for software claim drafting, these new claim formats should be used with care. The true benefits of these formats are almost as transient as the carrier waves on which they were founded. It

will be a rare instance when the scofflaw infringer in Sealand[61] will bow to a U.S. injunction to stop providing downloadable information to clients in the U.S.

Given the challenges that enforcement may entail, any equitable remedies won may not be worth the paper they are written on. Still, there may be some defensive life left in these new claim formats even if the likelihood of offensive utility is slim. Software companies seeking to cross-license with foreign companies may have new grounds for using their U.S. patents as bargaining chips in their negotiations.

Further, the cost of acquiring the benefit of the increased claim scope provided by propagated signal claims may be insignificant. Existing computer readable medium claims usually do not need to be modified, and only minor modifications to the patent specification will give those claims support for propagated signals as one of a myriad of computer readable media.

Propagated signal claims may not be a new layer of armor for protecting software patents, but they do fill a few of the chinks in the existing armor.

---

[61] Ann Harrison, *Data Haven Says It Offers Freedom From Observation*, ComputerWorld, November 13, 2000, p. 50.