EXHIBIT A

Part IV – Content Identification[1]

As this article has been considering certain intellectual property ramifications relating to the transmission of content, it is important to consider how content can be identified (e.g., tracked for such purposes as collecting royalties) in the course of its transmission. A starting point in an analysis of "content identification" with respect to wireless networking technology, and in particular, the role of the IEEE standard 802.11, is an understanding of what is meant by "content." This has important ramifications for intellectual property owners and information systems developers alike. Further, the use of higher level identifiers to authorize or coordinate simple lower level functions such as "change status to activate or not" may assist in the provision of digital information and other digital goods and services that may be subject to intellectual property restrictions;

and such identifiers may also be required for the management of more complex types of wireless networking operations.

Despite the unfortunate tendency to view "content" as restricted to traditional copyright works, whether "born digital" or converted to digital form, a much wider variety of digital "content" is being implemented in a network environment. These new resources are likely to involve the application of bodies of law other than copyright, such as patent, securities, banking, insurance, and communications. When organizing and deploying identifier systems at lower 802.11 levels, care should be taken to accommodate the interaction between 802.11 identifier systems and new forms of "content." Examples of such content might be one or more virtual

[1] Contribution of P.A.Lyons, Committee 703--Spring Report (2003), American Bar Association.

machines implemented at various points in a 802.11 network, as well as the static and dynamic relationships of such information management systems or other identifiable elements in the Internet or other networking environment. For example, much effort has been expended on the development of various computational facilities known as “virtual machines;” and these facilities are being used to perform various operations for a wide variety of home and business applications. Where such virtual machines interact with information elements in an underlying 802.11 physical layer, manage access to external digital resources or perform other “stated operations,” these computational facilities may themselves be viewed as “content.” The interaction of identifiers assigned to this new form of "content" at various levels of granularity, as well as the identifiers used for more traditional copyright resources, and the interaction of any such identifiers with lower level 802.11 information elements, is an important area for further consideration within the IEEE 802.11 standards process.

Where content providers have developed digital asset management systems to identify their digital goods and services, including specialized metadata and related rights management technology, the tracking of such good and services may be important for owners of intellectual property rights. Several concepts used in 802.11 may require reassessment to accommodate this development. In particular, the medium access control (MAC) management capability is an example of an 802.11 specification that may require adjustment. For example, as described in the IEEE 802.11 Handbook by Bob O’Hara and Al Petrick (1999), at page 101, “dot11StationID is a 48-bit attribute that is designed to allow an external manager to assign its own identifier to a station, for the sole purpose of managing the station.” Where an access point or “station” is an element in a distributed information management system, either entity could come within the meaning of the 802.11 standard, or parts of it could be relegated to the status of an 802.11 higher level protocol. From a content viewpoint, various software capabilities now typically treated as higher level protocols in the IEEE 802.11 standard could also be viewed as part of the access point or station in 802.11 terminology.

While the issue of digital asset management might be seen as unimportant to the developers of wireless networks, whose focus may only be on communications connectivity, it could be of real concern to owners of content who may have no other effective recourse to monitor or verify compliance with terms and conditions placed on specific digital information goods or services. The ability for a sufficiently endowed (i.e., with powerful computer resources) unauthorized "outside party" to tap into an 802.11 network, effectively subverting normal security provisions, is clearly within the realm of possibility. If such concerns become prevalent, it may be desirable to assign some form of identifier external to the 802.11 specification to each transmitted frame, or specific elements of a frame, so that the identifier can be used to maintain records of authorized transactions or to track any unauthorized use or interception back to its source (indeed, a "frame" may itself be viewed as a structured information resource in this context, i.e., content with its own identifier and stated operations).

A question may also be raised with respect to other information elements and associated element identifiers set forth in 802.11 (Id. at 67). Any identifiers or other metadata associated with "access points," "stations," "MACs," "frames," or other 802.11 compliant elements, could be made known to digital information management systems, or mutually trusted third parties, and steps taken to coordinate such 802.11 identifiers with identifiers associated with "content," whether or not such identifiers are external to the 802.11 standard. This would appear to be a useful step toward encouraging the development of commerce based on wireless networking technology where intellectual property, security, privacy or other restrictions apply.

At the present time, virtually all computer-based communication systems involve moving bits from a source to one or more destinations (in the latter case this may occur by broadcast or selective multi-cast as well as multiple one-to-one interactions) without regard to the meaning of the bits being communicated. For purposes of content identification, it would be most useful and practical to identify content at higher levels than either 802.3 or 802.11 now appears to allow. For example, if content capable of being independently identified and processed was present in the form of a digital object, i.e., structured data having an associated unique persistent identifier, then it would be possible to track content at various points in the communications pathway, or even identify transaction records at such points. However, since actual content may be encrypted in different networks or, more generally, in different information systems, explicit arrangements would have to be made with the system operators to leave the identifier field in the clear (if, indeed, the 802.11 standard would allow this when encryption is used), or to trust various intermediary systems along the way that see the content in the clear to extract the identifiers for the purpose of content identification and processing.

At best, this is a very sensitive matter. Any such arrangements would have to be built into agreements with the originators of the content and managed within the overall communications environment. This may be accomplished through such means as associating specific terms and conditions with individual digital objects in a form that is interpretable along the way so that appropriate decisions can be made on the performance of permitted operations such as further dissemination, reproduction or aggregation. An example of an identification/resolution system that can assist here is the Handle System (see www.handle.net).

The assignment and use of identifiers associated with digital objects and other digital resources is an important area of research. Some progress has been made in this context, but much remains to be done. Coordination of these efforts with the IEEE 802.11 standard development process, and related efforts, is desirable. While 802.11 may be viewed by some as too low-level a system to encumber with this kind of baggage, certain basic identification elements might be desirable at that level to authenticate information systems and other digital resources in order to facilitate verification and compliance with approved “stated operations” for each digital object or other digital resource (whether also viewed as a “MIB,” "communication" or "frame") without violating any confidences or other restrictions placed on the material. It is also important to provide a logical distributed connection between any such lower level identifiers with intermediate management system identifiers, e.g., URI’s or other names assigned to various elements in one or more virtual machines that may be connected with an 802.11 computational facility, and, ultimately, with identifiers and other metadata that may be associated with information elements by intellectual property owners or their agents for purposes not just of delivery of digital objects or other digital resources, but to enable a wide variety of stated operations to be performed on such objects on a static or dynamic basis.

In summary, at a minimum, there is a need for visibility between higher level identifiers and those assigned at lower levels such as MAC addresses, as well as the coordination of these identifiers and related metadata with network system elements such as IP addresses. This may take the form of simple methods for tracking and accounting of identifiable digital information in order to facilitate the enforcement of contractual restrictions on material subject to intellectual property, or the detection of unauthorized external intrusions.