LEGAL ISSUES IN A TRUSTED DOMAIN[a1]

by David St. John-Larkin[a2]
edited by Jud Cary[a3]
Cable Television Laboratories, Inc.

Abstract

A Trusted Domain generally provides for the delivery, retention and utilization of copyrighted content within a secure residential network. This paper attempts to identify and to address some of the key legal issues of copyright law that are presented in a Trusted Domain in the abstract sense. An in-depth discussion of technical and business issues raised by Trusted Domains is beyond the scope of this paper.

Contrary to those commentators who criticize trusted systems as parochial or limiting,[1] the thesis of this paper is that the Trusted Domain can (1) preserve, if not increase, current copyright law privileges enjoyed by consumers, (2) assure content owners of a secure network and (3) provide distributors a new product offering. Ultimately, the Trusted Domain may serve as a model for the next generation of content-related services that preserves the expectations of consumers, and protects the rights of copyright owners alike.

I. INTRODUCTION

The digital world of the 21st Century is no different than Alice's Wonderland.[2] In both cyberspace and the fictional land at the end of a rabbit's hole, there exist communities that do not rely upon the scientific laws of nature or real-world social and legal norms. Just as an invisible cat makes sense in a world of talking playing cards, a "worm" that unobtrusively embeds itself within vulnerable computers to monitor suspicious activity makes sense.[3] In other words, the laws governing both worlds are entirely self-imposed. In Alice's world the Queen of Hearts (presumably) sets forth the law, in the digital world "*code is law*."[4]

One key attribute of "code," including copy control software and digital rights management systems (DRMs), that underlies our digital world is that it is mutable. Code is not bound to follow rigid structural or architectural guidelines; rather, code is flexible and can adapt to new or changing circumstances. A second important attribute of code is that it can facilitate fast distribution of perfectly replicated information. These attributes have led some to proclaim the vision of a technological utopia, a modern Enlightenment where individuals share information, knowledge, and culture at the press of a button or pulse of light.[5] Some commentators, however, offer that code leads to a "dystopia [where] digital technology is the handmaiden of copyright infringement" and the death of copyright law.[6] The fear expressed by these commentators is that digital technology will supplant copyright law, and that owners of digital content will use code to "undermin[e] the utilitarian balance of copyright [law] and threaten free expression."[7] While not entirely unfounded, these fears are reactionary. It is certainly true that code or digital technology could be used to usurp the general provisions of copyright law. Conversely, code could strictly enforce copyright law and restrict traditional fair use privileges that most consumers in the digital world now assume as a right.

As originally suggested by Mark Stefik, the concept of trusted systems offers a model for code to exercise complete control of digital content.[8] The protection of digital content from unlawful distribution, especially in the post-Napster age of peer-to-peer networking (e.g., KaZaA), is an important reason to implement trusted systems. However, the existence of a trusted system does not of itself eradicate the privileges bestowed by copyright law. This paper discusses a type of trusted system, called the Trusted Domain, that can preserve, if not increase, copyright law privileges enjoyed by consumers while concurrently assuring content owners of a secure network. Because trusted systems rely upon code, the Trusted Domain can flexibly incorporate and closely model copyright law, as well as appurtenant copyright privileges such as fair use. Moreover, there is ample reason why the Trusted Domain should be crafted to model real world copyright law. Simply stated, Americans love fair use–fair use privileges are marketable goods that increase the value of content to the consumer.[9]

This paper discusses the Trusted Domain as applied in the context of a home network consisting of a plurality of multimedia components (see Illustration A., below). Part II sets forth the general architecture of the Trusted Domain, and describes the possible range of specific characteristics a Trusted Domain may implement. Part III explains how the Trusted Domain affirms, rather than annihilates, certain copyright law principles, including the first sale doctrine and fair use, and may even be used to preserve or enhance certain privacy protections. This paper concludes by submitting that the libertarian Trusted Domain protects digital content and ensures the continuation of copyright privileges that are consistent with the expectations of both content owners and consumers alike.

II. ARCHITECTURE OF THE TRUSTED DOMAIN

Conceptually, trusted systems consist of a set of protocols or rules[10] that govern the use, management and protection of copyrighted material. Physically and logically the Trusted Domain is embodied in a network architecture[11] that can include various rules or functions related to the use of content in the Trusted Domain, including the backup,

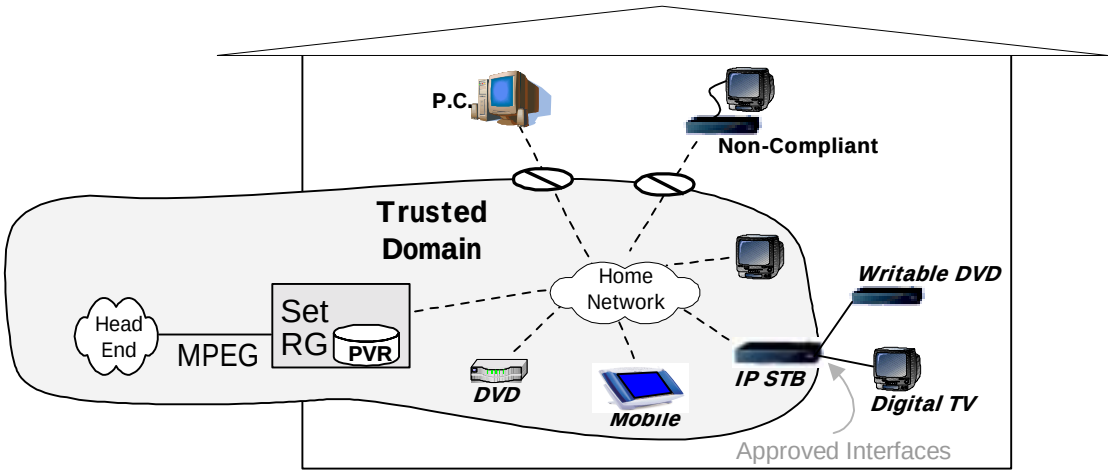

Illustration A.

conversion, distribution, playback, recording, storage and transport of copyrighted material. The most important attribute of a trusted system, implied by its name, is that it must identify Trusted and Non-Trusted Devices.[12] A Trusted Device is an application or electronic device capable of identifying itself and implementing the rules of the Trusted Domain. Likewise, a Non-Trusted Device is any application or electronic device that does not identify itself or cannot implement the rules of the Trusted Domain.

Any set of Trusted Devices or Non-Trusted Devices may be combined into a Trusted Domain.[13] The purpose of a Trusted Domain is to enforce rules applicable to individual Trusted and Non-Trusted Devices. Importantly, a Trusted Domain must establish, manage and enforce rules for each device connected within the domain. In other words, the set of Trusted Devices that comprise the Trusted Domain must establish trust within the network and maintain a secure means of managing the input and output of content within the Trusted Domain.[14]

A. Usage Rules

Content usage rules imposed upon the Trusted Domain can generally be divided into two categories: distribution (or transport) rules and content rules. Distribution rules enable the Trusted Domain to verify that content is transferred only to devices implementing the requisite security safeguards, e.g., transfer to other Trusted Devices. Content rules enable the Trusted Domain to implement requisite control over the content that is utilized by a Trusted Device. The content usage rules of a Trusted Domain are entirely self-imposed. Because they generally rely upon code, the content usage rules imposed upon Trusted Devices are customizable and may be as restrictive or unrestrictive as necessary. As discussed in the following subsections, there are two fundamental paradigms for asserting content usage rules within a Trusted Domain: the libertarian Trusted Domain and a rule-based Trusted Domain.

B. The Libertarian Paradigm

One embodiment of the Trusted Domain implements only a single, simple, content usage rule: within a Trusted Domain there are no content or distribution rules, apart from the requirement that content only be distributed to other Trusted Devices. This open or libertarian paradigm builds upon the assumption (set forth above) that a Trusted Domain is able to identify and regulate the connection of Trusted and Non-Trusted Devices to the network. Subject to initial access and authentication of Trusted Devices, in this simplified form, a Trusted Domain would eliminate the need for complicated copy control and content encoding rules. Within the secure network of a Trusted Domain, a person would then be free to use and distribute content without restriction: any content, any time, anywhere within the Trusted Domain.

For example, a person could distribute a movie purchased for the Trusted Domain to all Trusted Devices capable of video-playback that are within the Trusted Domain.[15] Instead of restricting playback of the movie to a single DVD player, a person could simultaneously transfer or play the movie on other Trusted Devices such as a personal video recorder (PVR), LCD projector or the digital television on the front of your refrigerator. Furthermore, use of a movie within the libertarian Trusted Domain would also be free of any copy control restrictions (e.g., copy-once, copy-never,

view-only, view-once, etc.). Instead, the movie could be freely consumed and used within the Trusted Domain. So long as the content remains within the Trusted Domain, the content can be utilized without restriction.

For simplicity, and for the purpose of raising and discussing general legal topics, this paper focuses on this "libertarian" version of a Trusted Domain–once within the Trusted Domain, content is generally available any time, anywhere within the Trusted Domain. Of course, a wide variety of distribution and content rules, and every combination thereof, could be imposed on a Trusted Domain system. And, different technical or business considerations may influence a particular desired Trusted Domain. However for academic discussion, those issues are outside the scope of this paper. Section III of this paper therefore proceeds to address the legal significance of this libertarian model in greater detail.

C. The Rule-Based Paradigm

An alternative to the libertarian Trusted Domain is a rule-based Trusted Domain that implements one or more rules to control or to regulate the use and distribution of content within the Trusted Domain. In contrast to the libertarian paradigm, the rule-based paradigm establishes a set of rules to regulate any or all of the activity within the Trusted Domain. Various functions could be made subject to such rules, including backup, conversion, distribution, playback, recording, storage and transport of content. Various rule-based paradigms already exist in the digital domain. For example, content "Encoding Rules" are required when using the Digital Transmission Copy Protection (DTCP) system (e.g., on a 1394 digital connector). Copy protection schemes that exist in physical media can also be honored or modeled in a Trusted Domain; for example, CSS protection on a DVD, or the various copy protection methods applicable to CDs could be enforced in the rule-based Trusted Domain.

Although existing copy protection rules can be modeled in the Trusted Domain, it is arguable that content owners might be more willing to "soften" such rules within the Trusted Domain because they know that the Trusted Domain network is secure, and is limited to the Trusted Devices on the Trusted Domain. This reasoning may especially hold true in a Trusted Domain limited to the home environment where the number of Trusted Devices is relatively small, and the audience is limited. In other words, copy protection rules that apply to a particular piece of content outside the Trusted Domain may differ from the copy protection rules that are applied to the same piece of content within the Trusted Domain. The rule-based Trusted Domain paradigm offers a wide variety of options to content owners, distributors and consumers. As expected, the technical and business issues are also more complex. For simplicity, this paper focuses on the libertarian Trusted Domain noted above. However, many of the core legal issues remain the same.

III. COPYRIGHT LAW AND THE TRUSTED DOMAIN

The libertarian Trusted Domain paradigm (or even a rule-based Trusted Domain with fairly lax copy protection rules) has the potential to preserve in the digital domain two fundamental copyright law principles: the protection of copyrighted content, and the preservation of fair use privileges. Additionally, the distribution of copyrighted content within this paradigm comports with the first sale doctrine by allowing the consumer to freely distribute content to other

Trusted Devices. The Trusted Domain also may preserve, or even enhance, certain privacy expectations. The following subsections discuss the legal implications of the libertarian paradigm for the protection, use and distribution of content within the Trusted Domain.

A. The Trusted Domain as a Compliment to the Law

The protection of copyrighted content is typically accomplished via *ex ante* or *ex post* enforcement measures. Generally speaking, technical prophylactic measures protect content *ex ante*, whereas legal enforcement measures protect content *ex post*.[16] Technical prophylactic measures include the use of encryption, third-party verification, device and user identification, self-healing software and digital certificates (that may be embedded in silicon). Legal enforcement measures include the use of contract law, copyright law, and the anti-piracy (anti-circumvention) provisions of the Digital Millennium Copyright Act. The Trusted Domain, and trusted systems generally, are best classified as a technical prophylactic measures:

> Trusted systems . . . achieve what copyright law achieves. But [trusted systems] can achieve [copyright protection] *without the law doing the restricting*. [Trusted systems] present a much more fine-grained control over access to and use of protected material than law permits, and it can do so without the aid of the law.[17]

The general distinction between *ex ante* and *ex post* copyright protection, however, does not suggest that code and law are substitutes. *Ex ante* enforcement must be responsive to the immediacy of potential copyright infringement. In a world where data can be instantaneously replicated and transmitted, legal protection is much too slow. On the other hand, technical measures gain legitimacy through the law and the law is much better equipped to sanction people who try to infringe upon copyrights. The use of technical and legal measures to protect content therefore establishes a complementary or symbiotic relationship. Some commentators downplay the differences underlying this relationship and suggest that code and law are substitutes in their protective ability.[18]

The Trusted Domain, as an *ex ante* copyright protection mechanism, is a necessary and unique compliment to the legal protections afforded by the Copyright Act of 1976 (Copyright Act) and, as amended, by the Digital Millennium Copyright Act (DMCA).[19] The Trusted Domain implements a flexible, but still robust and secure, transport layer that rides on top of a network layer (e.g., a hybrid fiber-coax cable plant).[20] If history is our guide, however, it is apparent that technological safeguards will "probably not be 100 percent effective."[21] The Trusted Domain, by implementing multiple renewable copy protection mechanisms (enumerated above, e.g., digital certificates), implements a corrective means of quickly resolving potential security holes.[22] Because the circumvention of technological copyright protection measures implicates the reproduction right,[23] Congress passed the DMCA as a complementary *ex post* legal enforcement regime.[24] Section 1201 of the DMCA prohibits the manufacture and distribution of devices (and the rendering of services) for the purpose of circumventing technological measures that protect against unauthorized access to works.[25] So, Section 1201 addresses the conduct of circumventing a technological measure that protects

access.[26] Congress passed this *ex post* enforcement measure because it recognized the urgency and importance of protecting digital content: once digital content is copied, it is very easy to duplicate and distribute.[27] The effect is that Section 1201 publicly discourages the circumvention of copy protection measures through the threat of an *ex post* application of copyright law.

Another complementary *ex post* copyright enforcement measure is provided by contract law. Generally speaking, contract provisions governing aspects of copyrighted works are enforceable.[28] There is, however, disagreement among courts as to the scope of "specific contractual provisions that would otherwise be enforceable under state law."[29] An expansive interpretation[30] of Judge Easterbrook's opinion affirming "shrink-wrap" licenses in *ProCD, Inc. v. Zeidenberg* highlights this disagreement, and distinguishes state contract rights from the exclusive rights in the federal copyright regime:

> Rights "equivalent to copyright" are rights established by law–rights that restrict the options of persons who are strangers to the author. . . . A copyright is a right against the world. Contracts, by contrast, generally affect only their parties; strangers may do as they please, so contracts do not create "exclusive rights."[31]

Thus, bilateral contracts, contracts that exist between two parties, "may be enforced."[32] As it pertains to preventing the circumvention of trusted systems, contract law thus provides the Trusted Domain with another means of enforcing copyright protection measures beyond technical safeguards. Establishing contracts that define the boundaries of permissible behavior within the Trusted Domain provide yet another tool to safeguard content and reinforce *ex ante* technical content protection measures. However, as explained below, contract restrictions in the digital world may encroach upon traditional first-sale concepts and thus may diminish the value of content in the Trusted Domain without adding any more protection to the content than is already incurred by the use of other *ex ante* and *ex post* copy protection measures.

B. The Trusted Domain and Benefits of the Fair Use Doctrine

The libertarian Trusted Domain may preserve, if not expand, the fair use privileges enjoyed by consumers in the analog world and respond to the difficulty of post-sale fair use valuation problems that were historically left unaccounted for by market pricing mechanisms. The Copyright Act grants copyright owners six exclusive rights, generally enumerated as: adaptation (derivative works), distribution, display, performance, reproduction and convergence (digital performance and transmission rights).[33] Fair use is a defense that can be asserted where there is infringement of one of these six exclusive rights.[34] The doctrine of fair use is highly contentious and was at one time labeled "the most troublesome doctrine in the whole law of copyright."[35] At the heart of the fair use doctrine is an ongoing debate about whether the doctrine is itself dependent and restricted by technology and subject to economic constraints imposed by the market forces. This debate is stereotypically between copyright owners, who regard the fair use doctrine as an artifact of the analog or print world that should slowly recede with time, and consumers, who view fair use as an immutable right that is necessary for promulgating one of the Copyright Act's purposes to convey copyrighted content back

into the public domain.[36] Copyright owners, in this generalized sense, assert that fair use only applies where the "transactions costs associated with clearing rights sometimes exceeded the value of the proposed use."[37] Consumers, alternatively, would claim that fair use is core to the principle establishing copyright laws in the first place–i.e., to benefit the public–and is "not merely a matter of economics" nor of technology.[38]

The rule-based Trusted Domain paradigm, as a means of regulating or controlling the specific use and distribution of content, may perpetuate the same quandary presented in this fair use debate. Rule-based usage rules permit the copyright owner to price the use of content on a *pro rata* basis.[39] Accordingly, the hypothetical copyright owners would say that the increased technological capability to control use piecemeal does not run contrary to the fair use doctrine:

> Fair use, [the copyright owners] argue, defined rights in an area where it was not possible to meter or charge for use. In that context, fair use set a default rule that parties could always contract around. The default rule was that use was free.
>
> But as the limits of what it is possible to meter and charge for changes, the scope of fair use changes as well. If it becomes possible to license every aspect of use, then no aspect of use would have the protections of fair use. Fair use, under this conception, was just the space where it was too expensive to meter use.[40]

Alternatively, the hypothetical consumers would state that the fair use doctrine is "inherent in the copyright – required whether technology makes it possible to take it away or not."[41] As presented below, the libertarian Trusted Domain paradigm not only recognizes these divergent positions, but presents a model much better suited to reconcile them.

The libertarian Trusted Domain paradigm fundamentally allows unrestricted use of content within the Trusted Domain. A book could be paraphrased within an electronic document, a movie clip embedded within a home-movie, or a song transformed instantaneously to play on multiple devices simultaneously. Assuming the actual use otherwise satisfies the other parameters of fair use,[42] the possibilities are endless. Another premise of the Trusted Domain, that all use within the Trusted Domain will not be metered or charged, assures the consumer that their fair uses continue unencumbered by *pro rata* licensing fees and protects that individual's personal content. This model, however, is also structured to protect content by assuring copyright owners that it remains solely within the network of Trusted Devices. Moreover, the libertarian Trusted Domain paradigm recognizes the legal importance and the monetary value of fair use by allowing copyright owners to set initial distribution prices at the convenient point-of-sale entry to the Trusted Domain and thereby capture the marginal costs of fair uses that were previously considered a market failure (and thus allowed free of charge).[43] Certainly, Americans love fair use. Instead of punishing or restricting fair use, the libertarian model markets fair use and creates new business models.[44] Ultimately, then, the libertarian Trusted Domain paradigm allows consumers to continue to enjoy their fair use privileges while providing content owners a convenient mechanism to set a price for fair use in a secure environment.[45]

C. The Trusted Domain and Preservation of the First Sale Doctrine

The libertarian Trusted Domain paradigm provides copyright protection measures that do not preclude application of the first sale doctrine. The first sale doctrine relates to the distribution right and is a limitation that prohibits a copyright owner from exercising control over the distribution of a tangible copyrighted work past the first-sale. In other words, a copyright owner may attach conditions on the first-sale of a copyrighted work (e.g., payment of a specific price) but may not thereafter condition resale or further distribution of the tangible copyrighted work upon any criteria. The first sale doctrine is a default rule "origin[ating] in the common law aversion to limiting the alienation of personal property" and policies opposing restraints of trade.[46] Codified in Section 109 of the Copyright Act, the first sale doctrine heralds back to *Bobbs-Merrill Co. v. Strauss*[47] in which the U.S. Supreme Court "construed the exclusive right to [distribute] . . . as applicable only to the initial sale, so that absent an appropriate contractual provision, there could be no restriction on re-sales."[48]

In the days of the *Bobbs-Merrill Co. v. Strauss* case (1908), the first sale doctrine was also practical to implement with respect to the media of the day – books, newspapers, etc.[49] Historically speaking, it was difficult or impossible to monitor further sale or distribution of such copyrighted works, or to collect compensation for such. However, with the advent of code, further distribution of copyrighted works can be easily tracked, monitored and regulated subject to technological controls. And, in some cases, such information can prevent further distribution or use of a copyrighted work, e.g., digital content marked "view-only" would also prevent any further distribution.[50] The distribution of digital content, however, can be fundamentally different than the distribution of books or other analog media. Where distribution of the digital content itself necessarily requires creation of a copy prior to distribution, "[S]ection 109 does not apply to [the] digital transmission of works."[51]

The libertarian Trusted Domain paradigm somewhat restores the historical and distribution-specific conception of the first sale doctrine, at least in spirit. Whereas a rule-based Trusted Domain may attach conditions that restrict the distribution of content to certain Trusted Devices, the libertarian model allows distribution to all devices within the Trusted Domain. Notably, to truly comply with the first sale doctrine, "distribution" in this sense would technically need to be a "move." That is, in the operation of transferring content, the storage place of the original content would need to be deleted or rendered unusable. [52]

Enabling the first sale doctrine through the libertarian Trusted Domain allows consumers to make use of digital content no different than how analog content, or books (with respect to further distribution, not copying), are utilized in the real world. Moreover, with the addition of a few simple content rules, consumers could distribute digital content to other Trusted Domains implementing the same management paradigm. Thus, the entrance to the libertarian Trusted Domain acts as the point-of-sale to provide the bargained-for uses that the first sale doctrine originally enabled under earlier technological constraints.

C. The Trusted Domain and Privacy

The advent of trusted systems prompted many commentators to reexamine the role of privacy norms in the digital world.[53] One

early commentator suggested that "the freedom to read, listen, and view selected materials anonymously should be considered a right protected by the First Amendment . . .."[54] The commentator also argues that the civil and criminal enforcement provisions of the pre-DMCA legislation may prove susceptible to constitutional challenge.[55] Trusted systems were seen as a form of "private legislation" that could potentially disrupt the balance between preservation of a copyright owner's exclusive rights and enrichment of the public domain.[56] Trusted systems, it was argued, could potentially marginalize, if not entirely eviscerate, copyright law.[57]

Contrary to these and other dire predictions forecasting the end of copyright law, more recent commentators noted the practical benefits that may arise by allowing trusted systems to manage consumer information. For example, automated information that covers the "provenance . . . and conditions of sale or license" may "substantially reduce . . . transaction costs."[58] Consumers and copyright owners also may benefit by a system that assures the authenticity and integrity of digital content delivered to the home.[59] Finally, it is now technically recognized that consumer-specific information can be anonymized. Anonymizing or aggregating an individual's preferences with the preferences of other people allows copyright owners and distributors to lower transaction costs, ensure the authenticity and integrity digital transmissions, while also directing sufficiently targeted information to consumers (e.g., targeted advertising).

The libertarian Trusted Domain may preserve, or even enhance, certain expected privacy norms. It is recognized that some *de minimus* form of metering must be established at the point of entry into the Trusted Domain in order to enable proper billing and payment.[60] However, once inside the libertarian Trusted Domain, no further metering is required; content may be used anytime and anywhere within the Trusted Domain. This is not to say, however, that consumers may not want more monitoring within the Trusted Domain. It is foreseeable, that given the option, many consumers may wish to monitor and store information to help backup and restore digital works or facilitate interactive services.

As such, we submit that the libertarian Trusted Domain may actually preserve certain expectations of privacy, now known in the analog world, in the digital domain.

IV. CONCLUSION

As this paper sets forth, the libertarian Trusted Domain paradigm protects digital content and recognizes the value of preserving copyright privileges that are consistent with the expectations of both copyright owners and consumers alike. The apparent benefits accruing from implementation of the libertarian Trusted Domain paradigm are numerous.

Consumers receive a convenient and standardized media platform that minimizes confusion about how to use content. This platform securely and transparently protects content within the Trusted Domain and preserves, if not expands, content usage expectations.

Content providers may also benefit from considerably more protection and security for the distribution of high-value digital content. The unrestricted nature of the libertarian Trusted Domain in particular increases the value of content, and allows content

providers and distributors to create flexible new business models to capture this value.

Likewise, consumer electronics manufacturers may benefit by a network that offers new market opportunities for devices and standardized interfaces for compatibility.

Finally, the Trusted Domain offers distributors a unique competitive network architecture for packaging and delivering content into the residential home.

In summary, the libertarian Trusted Domain can be used to affirm copyright law principles, including fair use privileges, establish a digital media platform that creates value to consumers, content owners, device manufacturers, and distributors.

[a1] The opinions expressed in this paper are that of the author and editor individually, and do not represent the opinions of the companies or industry in which they are employed.

[a2] Third-Year Law Student and Production Editor, Journal on Telecommunications and High Technology Law, University of Colorado School of Law. B.S., Environmental Studies & Social Policy, Northwestern University, 1997; B.S., Computer Science, *magna cum laude*, Michigan Technological University, 2002.

[a3] Assistant General Counsel, CableLabs. B.S., Applied Math & Computer Science, University of Colorado, 1986; M.E. Engineering Management, University of Colorado, 1993; J.D. *cum laude*, Santa Clara University, 1993.

[1] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 136-139 (1999); Yocchai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 418 (1999); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 981-82 (1996); Mark Gimbel, *Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law*, 50 STAN. L. REV. 1671, 1671-72 (1998).

[2] ROBERT LOUIS STEVENSON, ALICE'S ADVENTURES IN WONDERLAND (1865). In some cases, there is no distinction between the two worlds. *See e.g.*, *Alice in Wonderland – An Interactive Adventure!*, *at* http://www.ruthannzaroff.com/wonderland (last visited Mar. 9, 2003).

[3] LESSIG, *supra* note 1, at 17 (Lawrence Lessig offers the surveillance "worm" story as a means of showing how cyberspace is both like and unlike real space; the forced entry of a non-invasive worm may be so unlike the real world such as not to raise Constitutional eyebrows.).

[4] *Id*. at 7 (emphasis in the original).

[5] Mark Stefik, *Letting Loose the Light, in* INTERNET DREAMS: ARCHETYPES, MYTHS AND METAPHORS 220-21 (Mark Stefik ed., 1996).

[6] Gimbel, *supra* note 1, at 1671; John Perry Barlow, *Selling Wine Without Bottles: The Economy of Mind on the Global Net* (Dec. 1993) ("Copyright is dead."), *at* http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html.

[7] Gimbel, *supra* note 1, at 1671-72.

[8] *See* Stefik, *supra* note 5, at 220. The concept of trusted systems is discussed in Part II of this paper.

[9] To realize the value of maintaining fair use privileges, we need look no further than the rising popularity of personal video recorders (PVRs) such as those offered by Tivo or SonicBlue (ReplayTV) that allow television shows to be digitally recorded for later-viewing ("time-shifting").

[10] *See* Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us To Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137, 139 (1997).

[11] The network architecture of a trusted system is comprised individually or as a union of hardware and software.

[12] *See* Mark Stefik, *Trusted Systems*, SCIENTIFIC AMERICAN 78, 79 (Mar. 1997) ("[T]rusted computers have the capability to recognize another trusted system, to execute usage rights and to render works so that they either cannot he [sic] copied exactly or else carry with them a signature of their origin."). Discussion of the various technological tools used to verify trust are beyond the scope of this Article. Notably, the technological measures that verify trust must be renewable, revocable and robust. These characteristics generally require the implementation of self-healing (automatically upgradeable) software and silicon or embedded encryption safeguards.

[13] In computer science terminology, a Trusted Domain would most likely consist of a closed parallel network of devices communicating via an encrypted challenge-response system.

[14] *See* Stefik, *supra* note 5, at 229.

[15] As noted earlier, business models are outside the scope of this paper; but, query what the appropriate price for this type of a purchase for use within a Trusted Domain would be relative to other "traditional" purchases of the same movie, e.g., DVD movie rental, VOD.

[16] Citing a former research assistant's paper that attempts to discern the most efficient protections in cyberspace, Lawrence Lessig suggests that the real-world analog to the *ex ante* and *ex post* distinction is the difference between a fence and the law. LESSIG, *supra* note 1, at 122 (citing Harold Smith Reeves, *Property in Cyberspace*, 63 U. CHI. L. REV. 761 (1996)).

[17] LESSIG, *supra* note 1, at 129.

[18] For example, while Lawrence Lessig recognizes the possibility of this symbiotic relationship, he advocates that code currently displaces law:

> What copyright seeks to do using the threat of law and the push of norms, trusted systems do through the code. Copyright orders others to respect the rights of the copyright holder before using his property. Trusted systems give access only if rights are respected in the first place. The controls needed to regulate this access are built into the systems, and no users (except hackers) have a choice about whether to obey these controls. The code displaces law by codifying the rules, making them more efficient than they were just as rules. Trusted systems in this scheme are an alternative for protecting intellectual property rights – a privatized alternative to law. They need not be exclusive; there is no reason not to use both law and trusted systems. Nevertheless, the code is in effect doing what the law used to do. It implements the law's protection, through code, far more effectively than the law did.

Id. at 130.

[19] Copyright Act of 1976, 17 U.S.C. § 106 (1976); Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[20] *See* Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. Telecomms. & High Tech. L. 37 (2002) (offering a layered-model approach to understanding vertically-related communications platforms); *see also*, Douglas C. Sicker & Joshua L. Mindel, *Refinements of a Layered Model for Telecommunications Policy*, 1 J. Telecomms. & High Tech. L. 69 (2002) (suggesting that a layered model must incorporate the

technological characteristics of individual telecommunications platforms).

[21] U.S. COPYRIGHT OFFICE, *A Report of the Register of Copyrights Pursuant to §104 of the Digital Millennium Copyright Act*, 98 (Aug. 2001), *available at* http://www.loc.gov/copyright/reports/studies/dmca/dmca_study.html.

[22] The cost of developing sufficient copy-control mechanisms is not to be underestimated. Certainly the recovery of high fixed development costs would be difficult to recover, in the short term, if charged only to a single company's consumers. The economic rationale for development of robust security measures is better realized when internalized by a standard-setting organization.

[23] The Copyright Act provides that the copyright holder, or his or her agent, has the exclusive right to "reproduce the copyrighted work in copies or phonorecords. . . ." 17 U.S.C. § 106 (a)(1).

[24] U.S. COPYRIGHT OFFICE, *supra* note 21 at 98. Notably, Congress did not "prohibit the conduct of circumventing . . . [all] copy control measures," as this conduct may be permitted when claimed as a fair use defense, such as for library archival work. However, "fair use and other copyright exceptions are not defenses to gaining unauthorized access to a copyrighted work." *Id.* at 11-12. The analogy is clear: quoting a lawfully acquired book may be a fair use, quoting a book stolen out of a safe is not.

[25] *Id.* at 10.

[26] *Id.*

[27] STAFF OF HOUSE COMMITTEE ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, 2 (Comm. Print 1998) (Serial No. 6). The Senate Judiciary Committee explained that:

> Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy. Legislation implementing the treaties provides this protection and creates the legal platform for launching the global digital on-line marketplace for copyrighted works.

S. REP. NO. 105-190, at 8 (1998).

[28] Selby v. New Line Cinema Corp., 96 F. Supp. 2d 1053, 1059 (C.D. Cal. 2000) (courts have found, generally, that breach of contract claims are not preempted by § 301 of the Copyright Act).

[29] U.S. COPYRIGHT OFFICE, *supra* note 21 at 162.

[30] An alternative interpretation of Judge Easterbrook's *ProCD* opinion is that it limits "shrink-wrap" or "click-through" license terms past the first sale, only where there is full disclosure between the contracting parties.

[31] 86 F.3d 1447, 1454 (7th Cir. 1996) (citation omitted).

[32] *Id.*

[33] 17 U.S.C. § 106 (1996).

[34] The fair use doctrine was first articulated in *Folsom v. Marsh*, where Justice Story enumerated factors to decide issues of fair use:

> [W]e must . . . look to the nature and objects of the selections made, the quantity and value of the materials used, and the degree in which the use may prejudice the sale, or diminish the profits, or supersede the objects, of the original work. . . ."

9 F. Cas. 342 (C.C.D. Mass. 1841) (No. 4901). A full examination of the history and development of the fair use doctrine is

complex and beyond the scope of this paper. It is sufficient, herein, to note that Congress codified this judicial doctrine in § 107 of the 1976 Copyright Act, which sets forth four factors that are determinative of fair use:

> (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.

17 U.S.C. § 107.

[35] Dellar v. Samuel Goldwyn, Inc., 104 F.2d 661, 662 (2d Cir. 1939) (per curiam).

[36] U.S. CONST. art I, § 8, cl. 8 ("[T]o promote the Progress of Science and useful Arts, by securing for *limited* Times, to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.") (emphasis added). Another conception of the fair use doctrine was as a "proxy for a copyright owner's implied consent." Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 581 (1998) (citing MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 13.05 13-151 (disapproving of the notion) [hereinafter NIMMER]). Tom Bell notes that the proxy conception of fair use fell into disfavor because it did "not explain why fair use protects parody and other uses of copyrighted material that owners find disagreeable." *Id*. at 582.

[37] MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW § 10.17[A] (1999).

[38] *Id.*

[39] A proponent of rule-based usage controls, Jane Ginsburg states:

> As we move to an access-based world of distribution of copyrighted works, a copyright system that neglected access controls would make copyright illusory, and in the long run it would disserve consumers. Access controls make it possible for authors to offer end-users a variety of distinctly-priced options for enjoyment of copyrighted works. Were delivery of works not secured, novel forms of distribution would be discouraged, and end-users would continue to be charged for all uses, whatever the level in fact of their consumption.

Jane C. Ginsburg, *From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law*, Columbia Law School, (Public Law Working Paper No. 8, 2000).

[40] LESSIG, *supra* note 1, at 136 (citations omitted).

[41] *Id.*

[42] *See infra* note 34.

[43] Bell, *supra* note 36, at 581-84. Tom Bell notes that technology is more effective than fair use in responding to market failure. *Id.* Where transaction costs preclude value-maximizing uses of copyrighted content, "automated rights management radically reduces the transaction costs of licensing access to copyrighted works . . . it responds to market failure." *Id*. at 583.

[44] Responding to Lawrence Lessig's contention that a "small [ ] number of large companies" necessarily force consumers to choose restrictive usage architectures, David G. Post poses the rhetorical question:

> [I]f there are diverse architectures of privacy, of identity, and of content

> protection laid before the public, why is it so obvious that we will end up choosing the one(s) that deny us those things that Lessig (and I) think are so important?

David G. Post, *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace*, 52 Stan. L. Rev. 1439, 1454 (2000) (citing LESSIG, *supra* note 1, at 130.).

[45] A "property rights [regime, allows] the producer of intellectual property [to] charge more than marginal cost, and thus cover the total cost of producing and disseminating the works." J. Frank H. Easterbrook, *Technological Innovation & Legal Tradition: Enduring Principles for Changing Times*, 4 Tex. Rev. L. & Pol. 103, 105 (1999); *see also*, Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv. L. Rev. 1089 (1972) (presenting a framework for determining whether property, liability or inalienability rules should protect an entitlement).

[46] NIMMER, *supra* note 36 at § 8.12[A], fn 5 (*citing* Sebastian Int'l, Inc. v. Consumer Contacts (PTY) Ltd., 847 F.2d 1093, 1096 (3d Cir. 1988)).

[47] 210 U.S. 339 (1908).

[48] NIMMER, *supra* note 36, at § 8.12[B][1].

[49] Some commentators have called for the expansion of Section 109 to include digital works. U.S. COPYRIGHT OFFICE, *supra* note 21, at 40. The Office recognizes that, "*[p]hysical* copies of works in a digital format . . . are subject to [S]ection 109 in the same way as *physical* copies of works in analog form." *Id*. at 78 (emphasis added). However, this is *not* to say that digital distribution of the work itself—which generally includes copying, not just distribution of the physical medium—is intended to be covered under the ambit of Section 109.

[50] However, "[t]he first sale doctrine does not guarantee the existence of a secondary market [(called an aftermarket)] or a certain price for copies of copyrighted works." U.S. COPYRIGHT OFFICE, *supra* note 21 at 74 (responding to arguments that CSS technology limits the resale or aftermarkets for used DVDs). Furthermore, "[t]o the extent that there is a concern that region coding may limit the number of purchasers outside North America who are willing to buy [region-encoded] DVDs . . . that concern has nothing to do with § 1201 [of the DMCA]." *Id.* at 74, n. 263.

[51] *Id*. at 80. The U.S. Copyright Office explains why the reproduction right takes precedence over the distribution right, saying:

> The Supreme Court [in the *Bobbs-Merrill* decision] drew a sharp distinction between the two rights, creating an exception to the vending (i.e., distribution) right *only to the extent that it didn't interfere with the production right*.

Id. (citation omitted) (emphasis added). In fact, the *Bobbs-Merrill* decision explains this purpose, noting that "a grant of control to the copyright owner over resales would not further [the] main purpose of protecting the reproduction right." *Id.* at 20-21 (citing 210 U.S. 339 (1908) ("[T]he main purpose [of the copyright statutes is] to secure the right of multiplying copies of the work . . . .").

[52] It is noted that the DTCP encoding rules allow for such "move" operations.

[53] *See e.g.*, Cohen, *supra* note 1, at 982 ("[T]he new copyright management technologies force us to examine anew the sources and extent of that freedom."); Niva Elkin-Koren, *Copyrights in Cyberspace–Rights Without Laws?*, 73 CHI-KENT L. REV. 1155 (1998).

[54] Julie E. Cohen, *Some Reflections On Copyright Management Systems And Laws Designed To Protect Them*, 12 BERKELEY

TECH. L.J. 161, 185 (1997) (citing Cohen, *supra* note 1, at 1003-30.).

[55] *Id*.

[56] *Id.* at 163 ("[Copyright management systems] may enable both pervasive monitoring of individual reading activity and comprehensive 'private legislation' designed to augment–and possibly alter beyond recognition–the default rules that define and delimit copyright owners' rights."); Elkin-Koren, *supra* note 53, at 1186 (The "technological ability to restrict access to information . . . provide information suppliers with an inherent advantage over users . . . .").

[57] Echoing John Perry Barlow's claim that "copyright is dead," *see infra* note 6, Julie Cohen suggested that:

> Copyright owners . . . envision using [self-enforcing digital] contracts to secure–and redefine–their 'informational rights.' Within this vision of private ordering and technological self-help, contract law rather than copyright law is paramount. Limits on information ownership set by the public law of copyright are conceived as optional restrictions that can be avoided using appropriate contractual language.

Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1090 (1998).

[58] Jane C. Ginsburg, *Essay–How Copyright Got a Bad Name for Itself*, 26 COLUM.-VLA J.L. & ARTS 61, 70 (2002) (suggesting that § 1202 of the DMCA reduces transaction costs and increases transaction reliability).

[59] *Id*.

[60] Trusted Domains generally use some form of authentication to discern Trusted and Non-Trusted Devices. And, it is recognized that such authentication methods need to be sensitive to First Amendment privacy concerns. General technical techniques exist to ensure a base level of privacy, including the method of anonymizing or aggregating data to ensure anonymous use. w