

# Journal of Technology Law & Policy

 UNIVERSITY OF  
FLORIDA  
Levin College of Law  
141 Bruton-Geer Hall  
Gainesville, FL 32611  
(352) 392-4980



## FINDING FENCES IN CYBERSPACE: PRIVACY AND OPEN ACCESS ON THE INTERNET

Ethan Preston

Ethan Preston expects to receive his J.D. from the Georgetown University Law Center in 2001.

Cite as: Ethan Preston, *Finding Fences in Cyberspace: Privacy, Property and Open Access on the Internet*, 6.1 J. TECH. L. & POL'Y 3, <<http://grove.ufl.edu/~techlaw/vol6/Preston.html>>(2000).

---

### INTRODUCTION

#### A. LANGUAGE, FACTS AND THE LAW

The Internet challenges our legal system because it makes legal outcomes uncertain. Particularly, laws made to protect computers on the Internet and computer security are applied unpredictably. Novel situations always place unique strains on the law; the law is sensitive both to equity and language.<sup>[1]</sup> Law is based on language; law that diverges from the language that forms its base risks incoherence. Incoherent law is unpredictable. At the same time, facts develop and evolve much more rapidly than language, but injustice ensues if the law does not respond to changing circumstances.

This article assumes that legal decisions about the Internet will continue to be based in partially on property rights. Application of property rights to the Internet is important. Without property rights, computer owners may not be willing to connect to the Internet if

their computers can be abused without legal remedy. However, application of property rights to the Internet is also problematic. Much of the efficiency associated with the Internet derives from the Internet's open nature. Almost all use of the Internet involves the use of computers that are not one's own. A regime of untrammelled property rights would assign liability to nearly all uses of the Internet. Internet users would be at the mercy of computer owners' whims. Without some provision for open access, liability for violations for property rights will chill productive use of the Internet. To some extent, this is intuitive. Connecting to the Internet implies some willingness to permit others to interact with one's computer. The law must balance between property rights and open access on the Internet. A central assumption of this article is that a limited license must be implied by a connection to the Internet.<sup>[2]</sup> The central concern of this article is not whether interactions on the Internet are sometimes free of liability, but rather determining which interactions are a basis for liability and which are not.

To that end, this article argues that computer law could benefit from abstraction. Specifically, this article argues that computer security law would be more coherent and protect equity more predictably if it treated the Internet as if it were physical place--cyberspace. Of course, "cyberspace" is not a place, but a metaphor for a medium of telecommunication.<sup>[3]</sup> This article's argument may be counter-intuitive: abstraction usually obscures the facts on which the law depends.<sup>[4]</sup> Telecommunication will always be distinguished from physical presence, regardless of how similar an experience the two become. Legal doctrines that confuse the two would make the law less coherent, less predictable and therefore less efficient. But using cyberspace as a metaphor does not require that we confuse cyberspace with a real place, only that we make rules that approximate the effect of how our property rules would function if cyberspace were real. If we use the metaphor instead to classify the interests that must be protected and clarify when they are to be protected, it can simplify and unify the law. This makes the law more predictable and therefore more efficient.

The remainder of this section will argue that the law could profitably adopt the use of the cyberspace metaphor. Section II develops the metaphor, describing how it

accommodates the values of property, privacy and open access. Section III discusses some of the novel factual circumstances that necessitate use of the metaphor. Section IV will examine the potential impact of the metaphor in three specific areas of law:

trespass to chattels<sup>[5]</sup> lawsuits in context of Internet-connected computers, computer fraud laws, and the anti-circumvention provisions of the Digital Millennium Copyright Act.

## B. HISTORICAL USE OF THE CYBERSPACE METAPHOR

The metaphor of the Internet as a physical place is entrenched in our popular culture. Popular wisdom credits science fiction author William Gibson with coining the term "cyberspace."<sup>[6]</sup> Cyberspace referred to futuristic computer interfaces which graphically represented computers as physical spaces that accommodated data, represented by physical objects.<sup>[7]</sup> As a literary device, cyberspace may now be a somewhat hackneyed metaphor.<sup>[8]</sup> While popular use might imply a common understanding and therefore some utility, literary history provides a cautionary tale about investing too much in a metaphor.

Professor Lessig's *Code* argues that the interplay between both technical and legal regulation govern cyberspace.<sup>[9]</sup> For instance, Lessig makes a comparison between the cyberplaces of Harvard and the University of Chicago Law Schools. Harvard University requires network users to register their computers, so their users can be "licensed, approved and verified."<sup>[10]</sup> The University of Chicago permits anyone with an Ethernet connection to plug into a jack on the campus.<sup>[11]</sup> The University of Chicago permits anonymous speech, while Harvard effectively forbids it.<sup>[12]</sup> The difference in technical regulation of the Internet creates different legal implications. Throughout *Code*, Lessig refers to cyberplaces, extensively describing how their architecture is shaped but not explicitly addressing cyberspace as a metaphor.<sup>[13]</sup> A few other legal commentators have implicitly endorsed cyberspace as a metaphor.<sup>[14]</sup> If legal commentary about the

law and the Internet endorses this metaphor, perhaps it is efficient for the law to do so as well.

## C. THE LAW'S USE OF METAPHORS

Metaphors are incorporated into the law for the purpose of "set[ting] forth principles and dispens[ing] justice (i.e., equality) and provid[ing] predictability . . . or at least to create the impression that [courts are] principled."<sup>[15]</sup> Important examples include the "wall of separation between church and state"<sup>[16]</sup> and "sticks" that compose "the bundle of rights that are commonly characterized as property" in the context of takings cases.<sup>[17]</sup> Caution is merited in endorsing a metaphor. Some metaphors may successfully provide guidance or principles<sup>[18]</sup> but some fail to do so.<sup>[19]</sup>

Our legal system should use the metaphor of cyberspace because it is capable of providing guidance and clarifying the interests in sometimes confusing factual circumstances. Often complex factual situations can be easily conceptualized by metaphor. If this metaphor eases conceptualization and that ease in turn improves the predictability of liability, then the metaphor promotes legal efficiency. Moreover, this metaphor could provide more flexibility in allocating liability than statutory language. Statutory language suffers from its static nature; it never changes while it is applied against a myriad of factual circumstances. Section IV.B discusses this specific point in greater detail, comparing the cyberspace metaphor against computer crime laws.

## II. FINDING FENCES

### A. FENCES AND PROPERTY

The metaphor of cyberspace permits us to draw property lines and borders on the Internet. One of the central tenets of property jurisprudence is that property is the legal right to exclude others.<sup>[20]</sup> By defining which interactions with a computer transgress property lines in cyberspace (and therefore violate computer owners' property rights) the

law can assign liability consistently and promote equity without losing coherence.

Harold Reeves Smith argued that Internet-related law could be made more efficient when dealing with certain issues by allocating property rights to system administrators.

[21] He argued that property rights would be most efficiently allocated to system administrators because they would be most likely to provide de facto enforcement of those rights. [22] Hence, system administrators would be able to make most efficient use of property rights. This article is, in part, a modification of Smith's argument. The right to exclude should adhere to parties who have the ability to implement technical measures of exclusion, regardless of whether they are system administrators or not.

The Internet is like a physical place where people constantly wander in and out of other people's property, typically with the owner's permission. In the real world, fences provide obvious boundaries, which may be otherwise lacking. Fences efficiently coincide with limits of legal liability because fences provide notice that others are meant to be excluded from the property. Liability for climbing over fences is efficient because it is predictable; fences provide notice that property rights have been asserted. Exclusionary technical measures in cyberspace and fences in the real world share the same functions. The relationship between fences and property law supplies the first corollary to the developing metaphor. Liability attaches in cyberspace only when people jump over fences. In real world terms, computer owners should be able to assert their property rights (in the form of imposing liability) only when users have circumvented technical measures that should have prevented the litigated use. This rule engenders several benefits. Judicial efficiency is promoted when prospective plaintiffs are required to at least try to fix the problem themselves before turning to the courts. Also, exclusionary technical measures reinforce legal rules about property and they provide concrete notice of assertion of property rights. Finally, this corollary checks property rights and provides the proper balance between property rights and open access. One might object that it may be difficult to define precisely where fences lie or what exactly constitutes an effective technical measure. This objection is based on a misapprehension of the function of legal metaphors. No legal metaphor functions as a

formula which robotically provides legal results. Judges interpret, adapt and apply legal metaphors to the specific facts before them. Judges using metaphors decide cases, not the metaphors themselves. This metaphor is meant to provide judges and others with a vehicle with which to make decisions that account for open access and privacy, as well as for property.

There are several other valid objections to the metaphor. It is inadequate to define property rights according to notice given by owners to others. Notice does not suffice for several reasons. Basing legal rights on the assertion of legal rights simply begs the question. While people can assert rights that they do not have, they can also fail to assert rights that they should have. This is especially true in the field of computer security, where security violations often occur precisely because an owner or operator has not anticipated a particular activity. Failure to anticipate an activity usually precludes explicitly prohibiting them to others. Finally, situations arise where a owner might be able to erect technical measures that protect some property rights but those measures nevertheless fail to provide users notice that property rights are to be excluded.

Other sound objections could be made over technical measures defining property rights. It may not be possible to build fences or establish effective technical measures. Effective technical measures may be unreasonably expensive or unavailable altogether. Another potential criticism is that legal recourse would never be needed for perfectly effective technical measures. These are valid objections; any property system based on technical measures must be tempered by the practicality of implementing those technical measures. Property owners should only be penalized for failing to implement effective technical measures only where there are measures reasonably available. There is a subtle efficiency gain here. Potential plaintiffs, concerned that their claim might fail because they did not use effective technical measures, will investigate whether technical measures are efficient. The record of this investigation can be used to prove that technical measures would have been inefficient or ineffective.

## **B. PROPERTY AND PRIVACY**

Another set of concerns focus on how the law decides who gets to erect fences. Fences should not be built over neighbors' land. As this article elaborates in Section IV.C, technical measures used to protect copyrights can be quite invasive and controversial. At the extreme, a recent trojan/worm not only gave the trojan's user unlimited access to the host computer, but actually prevented the host computer from accessing anti-virus sites that could "cure" the host.<sup>[23]</sup> It is counter-intuitive that this "technical measure" corresponds to a just property interest. Just allocation of property rights require additional considerations.

The first consideration is that the law should protect computer resources. In the real world, it is not controversial that computers are chattels.<sup>[24]</sup> The legal consequences of physical interference with computers (like kicking them or stealing them) are easily predictable.<sup>[25]</sup> Liability for unauthorized use of computer resources, such as processing time and hard disk space, has long been a feature of computer law.<sup>[26]</sup> (Indeed, there is even a market for processing cycles that would otherwise go unused.)<sup>[27]</sup> In the real world, it is usually clear who owns what computer. The application of the cyberspace metaphor should not change the ownership of a computer.

The second consideration is privacy. A salient definition of privacy is the ability to control the flow of information about one's self and the ability to make meaningful choices about when information is disclosed. The metaphor of cyberspace is useful here because it accommodates property rights, which in turn imply privacy interests. Privacy and the proprietary right to exclude depend on each other in other contexts. The solitary application<sup>[28]</sup> of the Third Amendment<sup>[29]</sup> found that "privacy interest[s] arise . . . out of the use and enjoyment of property" and that privacy interests gave rise to Third Amendment property rights.<sup>[30]</sup> When illegal searches are suppressed because they violate "legitimate expectations of privacy," Fourth Amendment jurisprudence has found that those expectations can be based on property.<sup>[31]</sup>

In a medium that permits extremely low cost duplication and transmission of information, the ability to control information is important. This importance is reflected in the persistence of privacy as a theme in legal and media commentary on the Internet.<sup>[32]</sup> The protection of computer resources and privacy interests in the real world should "translate" into the protection of property interests in cyberspace. An individual Internet-connected computer provides a certain amount of space for data. That computer's resources, like its memory and processing power, provide space, or real property, in cyberspace. If an Internet-connected computer can be seen as providing space, then data, or information, that resides on that computer can be seen as movable property, or chattels. The protection of privacy interests on the Internet (the right to exclude others from an owner's data) is implicit in the protection of property interests in Internet-connected computers.

## 1. LAWS WHICH FUNCTION LIKE THE METAPHOR

Two federal laws provide models that closely resemble how the fences in cyberspace metaphor might be applied. These laws reinforce measures taken to protect the privacy of information or communication with civil and criminal liability. In this sense, they recognize efforts to exclude other and expectations that others will be excluded as "fences." These laws also treat "fenced-off" information like property, by punishing efforts to circumvent exclusive measures.

The Internet implicates individual's ability to control information flows at several places. The user may create information flows autonomously but unwillingly<sup>[33]</sup> or unwittingly, others may take information from his computer, and information sent to others can be taken in transit. American privacy laws are an ad hoc collection of very narrowly drawn laws that mainly address information autonomously disclosed.<sup>[34]</sup> One exception in this regard is the Electronic Privacy Communications Act (ECPA).<sup>[35]</sup> ECPA governs electronic communications<sup>[36]</sup> that are not readily accessible to the general public.<sup>[37]</sup> Title I of ECPA criminalizes the interception of wire or electronic communications and

the use or disclosure of such communications when the interception of such communications were known to be in violation of ECPA.<sup>[38]</sup> Title I also criminalizes the use of "devices" to intercept communications<sup>[39]</sup> and the manufacture, distribution, possession or advertising of devices whose main commercial use is the intercept wire or electronic communications.<sup>[40]</sup> ECPA provides persons whose communications are intercepted in violation of ECPA a civil cause of action.<sup>[41]</sup> Title II criminalizes unauthorized access (or access in excess of authorization) of a facility where electronic communications are stored as well as unauthorized disclosure of electronic communication.<sup>[42]</sup> ECPA rules for law enforcement exceptions for interception of electronic communications and disclosure of stored information<sup>[43]</sup> are remarkably complex but ultimately irrelevant to this discussion.<sup>[44]</sup>

The Economic Espionage Act (the federal implementation of trade secret law) governs the disclosure of information.<sup>[45]</sup> Specifically, the EEA provides penalties for the theft of trade secrets:<sup>[46]</sup> "all kinds of . . . information . . . if A) the owner takes reasonable measures to keep such information secret; and B) the information derives independent economic value, actual and potential, from not being generally known, and not being generally ascertainable through proper means, by the public. . ."<sup>[47]</sup>

The metaphor of fences in cyberspace would protect privacy in a manner similar to the ECPA and the EEA. All three recognize efforts to exclude others as the basis for rights to remedy. ECPA protects electronic communications which are not available to the public. EEA protects information that is valuable because it is unknown. ECPA reinforces the property rights of electronic communication facilities owners and the expectations of privacy for users of electronic communication systems. By providing criminal and civil sanctions against unauthorized access to private communication and information, ECPA provides users of electronic communications an effective right of exclusion. ECPA has already been used to protect the privacy of communications stored

on a web site in *Konop v. Hawaiian Airlines, Inc.*<sup>[48]</sup> Konop was involved with a dispute over his union's concession to management and had encouraged other employees to use of his web site to discuss alternate representation.<sup>[49]</sup> Access to the web site was limited by passwords and usernames issued to employees not in management or involved in union representation who agreed to abide by certain conditions (including not disclosing the web site's contents).<sup>[50]</sup> The court found an ECPA violation when a manager obtained a username and password from a pilot and perused the web site.<sup>[51]</sup>

### C. OPEN ACCESS

Again drawing on the metaphor, fences create enclosed areas. By implication, fences create areas within which people are free to wander. The gains from treating technical measures as if they were fences in the real world would be lost if liability attached to interactions between enclosed and unenclosed areas. The benefits gained from the notice function that the fences served would be lost because the application of the law would once again become unpredictable. Nor would the law benefit from the reinforcement of technical measures with which it did not coincide.

Harold Reed Smith also presented an open-system model of the Internet that did not reference boundaries but referenced "the actions taken in [c]yberspace--considering their consequences and apparent motivations."<sup>[52]</sup> Smith recognized that the Internet functioned best by sharing access to computing resources and facilitating communication between users.<sup>[53]</sup> Smith found that open-system would permit sharing of computing resources when boundaries between networks were "permeable."<sup>[54]</sup> Smith's open-system model further informs the cyberspace metaphor. There is precedent for adopting Smith's open-system model; courts have previously presumed implied licenses based on social custom. The Supreme Court presumed an implied license to use unenclosed land from common customs prevailing at the time of the settlement of the American West:

We are of opinion that there is an implied license, growing out of the custom of nearly a hundred years, that the public lands of the United States . . . shall be free to the people who seek to use them where they are left open and unenclosed . . . Of course the instances became numerous in which persons purchasing land from the United States put only a small part of it in cultivation, and permitted the balance to remain unenclosed and in no way separated from the lands owned by the United States. All the neighbors who had settled near one of these prairies or on it, and all the people who had cattle that they wished to graze upon the public lands, permitted them to run at large over the whole region, fattening upon the public lands of the United States, and upon the unenclosed lands of the private individual, without let or hindrance. . . . Everybody used the open unenclosed country, which produced nutritious grasses, as a public common on which their horses, cattle, hogs and sheep could run and graze. It has never been understood that in those regions and in this country, in the progress of its settlement, the principle prevailed that a man was bound to keep his cattle confined within his own grounds, or else would be liable for their trespasses upon the unenclosed grounds of his neighbors. Such a principle was ill-adapted to the nature and condition of the country at that time. [\[55\]](#)

As implied licenses to used unenclosed lands promoted the settlement of the West, a implied licenses to use computer resources and data stored on computers presumed from an absence of preventative technical measures promotes use of Internet. The article will return to comparing the Internet to the unsettled American West when it considers the application of the metaphor to specific laws.

## **D. METAPHORS FOUND**

In review, this article has explored four aspects of the cyberspace fences metaphor. First, conceptualizing computers as embodying physical space in cyberspace permits the law to adapt current rules about privacy and computer security in a way that would mirror the function of property rules in cyberspace. Secondly, the metaphor permits the law to posit fences in cyberspace that then permits the law to define property rights in cyberspace much more precisely. The third aspect is that property in cyberspace must be based on property-like interests in the real world, such as privacy or actual ownership of the computers and information stored therein. Fences should only be built on one's own land. The final aspect of the metaphor is a presumption of open access where no

property rights have been effectively asserted. The Internet can effectively be compared the early days of the West. Without a presumption of free access to resources that are not cordoned off by technical measures, many uses of the Internet are thrown into legal indeterminacy. The law would be much more invasive and unpredictable, and much less efficient.

With this expanded metaphor of cyberspace, the article can examine information flows on the Internet and technical measures that protect them. The next section will describe how cyberspace actually "looks." In Section IV, the article will examine how laws would apply to these information flows and will use the cyberspace metaphor to point out shortcomings in our laws and advocate different language and different applications.

### **III. INFORMATION FLOW ON THE INTERNET**

#### **A. AUTONOMOUS INFORMATION FLOWS**

The Internet is a single network using a common communication protocol communication: the transmission control protocol/Internet protocol (TCP/IP). Communicating across the Internet typically implies a TCP/IP connection, although there are exceptions. There are four different layers of communication within TCP/IP; the network interface layer, the internet layer, the transport layer, and the application layer.

[\[56\]](#)

The network interface layer, or link layer, is where electronic signals are sent and received over the wire. The electronic signals may be packaged in order to achieve compatibility with the hardware.

The internet layer, or network layer, is where the Internet protocol functions by routing packages of data, called packets. Packets consist of data that are being sent to or from the computers and "packaging." The packaging includes source and destination IP addresses. [\[57\]](#) IP addresses are the numeric designation of individual computers on the

Internet. Packets sent through the Internet are routed according to their IP address; they perform substantially the same function as mail addresses. The other important communication protocol used at this level is the Internet control message protocol (ICMP.) ICMP is used for two important diagnostic programs; ping and traceroute. Packets sent by ping are returned by computers that are connected to the Internet. Ping is used to establish whether particular IP addresses have computers associated with them and whether those computers respond. Traceroute functions in a slightly more complicated fashion, but its function is to return a list of every IP address that is used to route data in between the source and destination IP address. Traceroute is used to identify and diagnose networks.

The Transmission Control Protocol operates at the transportation layer, negotiating the transfer of data between applications and the operating system that controls the connection to the Internet. The TCP controls socket generation. Sockets consist of ports and IP addresses. Port are numeric designations that permit TCP to distinguish between data on the basis of their application. Port numbers permit the operation of several applications simultaneously. The transmission control protocol reconstructs data passed from the internet layer into segments, while breaking data passed from the application layer into segments. Segments have a socket number and a sequence number. The sequence designation permits TCP to ensure that all segments are received both at the local and remote computers and that the segments are ordered correctly. A process called a the three-way hand shake initiates data transfers in TCP. First, a client computer sends out a packet with a "SYN" flag. The server responds with a SYN packet that has a initial sequence number (ISN) and an ACK packet that acknowledges the clients request. The client computer completes the process with an ACK packet that carries sequence information.<sup>[58]</sup> The other major protocol at the transportation layer is the universal datagram protocol (UDP). The UDP does not attempt to guarantee the reception of segments; it is used to broadcast messages to computers on a local network in situations where reception is not critical.

The application layer is where the user actually interfaces with the computer and the network. Data passes from the user's input into the application, which passes it to the

transportation layer.

Interaction on the Internet requires certain levels of disclosure. The lowest common denominator of information flow on the internet is an IP address. Traffic to and from a user's computer will probably be logged (if not reproduced) by their local Internet access provider and the remote computer.<sup>[59]</sup> Public WHOIS databases can correlate IP addresses with the internet service provider responsible for those IP addresses.<sup>[60]</sup> The Internet access provider can then correlate a particular IP address (and possibly the time at which that particular IP address was assigned) with the login name of a user. The login name can they be correlated with billing or other such records that personally identify the user of a particular IP address.<sup>[61]</sup> While Internet access providers do not generally disclose the identities of particular IP addresses without legal prompting (that is, subpoenas), users' privacy is dependent on the policies of their Internet access provider.<sup>[62]</sup>

Naturally, there are exceptions. Proxy servers will accept packets from the local computer and substitute their own IP address as the source address in the packet headings that are sent to the destination computer. The result is that the remote computer will not log the user's actual IP address, but the proxy's IP address.

Nevertheless, the user's IP will possibly be logged by the proxy.<sup>[63]</sup> There are different kinds of proxies, including those that occur accidentally and those designed for anonymity, security or speed. Depending on the logging policy of the proxy, they can offer complete privacy to users or merely create an additional step in identifying a user.

Automation and graphical user interfaces (GUIs) increase user accessibility to computers and increase productivity. Unfortunately, automation and GUIs also mask the underlying mechanics of information flow on the Internet. Because web browsing and other activities are made transparent, users are unaware of information that is inadvertently exposed through their use of applications. A prime example is browsing the world wide web. Web browsers expose users to the risks of cookies, Java and

JavaScript and environmental checkers. Often, even the use of proxy servers does not eliminate these risks. While a user autonomously chooses to load a web page, the user may be unaware of how the browser is leaking information about them.

Cookies are small text messages that are saved either as discrete files or as lines in a single text file. They are used to identify recurring visitors and can be used to track users as they move across the Internet identifying a user every time he or she requests a web page that requires data from whomever set the cookie. This feature of cookies gives web advertisers the best vantage point to observe web users, because large advertisers provide images in many web pages across the Internet. The most prominent Internet-banner advertiser is most likely DoubleClick, Inc., a New York-based corporation. DoubleClick claims that its patented DART technology provides real-time profiling of users demographically identified by cookies.

In December 1998, [DoubleClick] received over 5.3 billion requests for the delivery of ads (impressions) generated by an aggregate of approximately 6,400 web sites of 570 Web publishers . . . According to Media Metrix, 45.8% of Internet users in the United States visited Web sites within the DoubleClick Network during the same month. [\[64\]](#)

DoubleClick's activities generated a consolidated lawsuit alleging that "DoubleClick Inc. improperly used or monitored confidential information of computer users in delivering advertisements on the Internet." [\[65\]](#) The federal claims of the lawsuit were dismissed on summary judgement in March, 2001. [\[66\]](#)

Java is a computer language written by Sun Computing. Mini-applications (applets) written in Java are stored on the remote web page and are run when browsers encounter the appropriate "tag" in the source code of a web page. Browsers download compiled Java applications and execute them. [\[67\]](#) JavaScript is a series of extensions to the HTML language designed by the Netscape Corporation and implemented by most modern browsers. It is an interpreted language designed to control the browser (as known as a scripting language, meaning that remote web server hosts the source code

and the source code is compiled by the client).<sup>[68]</sup> Both Java and JavaScript have a series of security issues<sup>[69]</sup> including permitting the discovery of a user's IP despite a proxy,<sup>[70]</sup> stealing files from a client computer and monitoring a user until sensitive information is revealed,<sup>[71]</sup> and the execution of arbitrary code.<sup>[72]</sup>

Browsers also reveal environmental variables in the header fields of the HTML language. Information revealed in environmental variables includes the user's original IP address, his browser version and operating system.<sup>[73]</sup>

Users can also inadvertently expose their IP address by opening documents with images supplied by embedded URLs. If a user is connected to the Internet, Microsoft Word<sup>[74]</sup> and email programs capable of displaying HTML will load the images from remote sites as if they were web browsers.<sup>[75]</sup> Indeed, documents with unique URLs could be prepared to track the viewing of a document across the Internet. Indeed, images consisting of a single pixel can be embedded in documents so that the document users would not know that they were loading images at all. Microsoft Word is also capable of writing and sending cookies that Microsoft Explorer keeps on a user's computer.<sup>[76]</sup> This could expand the potential threat to privacy.

## **B. EXOGENOUS INFORMATION FLOWS**

A connection to the Internet can reveal substantial information about a computer at the direction of a remote user. Pinging an IP addresses will reveal if that IP address is connected to the Internet and responsive. Although ascertaining the presence of computers at an IP addresses is necessary for the function of the Internet and may seem uncontroversial, many system administrators react negatively to systematic pinging by remote networks.<sup>[77]</sup> Other activity is even more invasive. Each platform and operating system has a unique "fingerprint" on the Internet, which can be found be

sending a series of specially crafted IP packets to a computer and comparing the responses (or lack thereof) to profiles of known operating system/platform.<sup>[78]</sup> Probably the best implementation of operating system/platform TCP/IP-based identification is nmap.<sup>[79]</sup> Nmap is also a port scanner.<sup>[80]</sup> Packets can also be sent to different ports to check if they are open (if applications are receiving data on those ports.) This technique is called a port scan; it also can be used to predict whether particular applications are running on a computer (although applications can usually be made to use arbitrary port numbers.)<sup>[81]</sup> Responsive applications have further implications. Some applications display a brief text message, or a banner, that announces the name and version of the application.<sup>[82]</sup> Collecting this information systematically called banner grabbing. This is significant because certain applications can only be run on particular operating systems. Finally, some applications will disclose the operating system at the prompting of unauthenticated users.<sup>[83]</sup>

Another class of disclosure occurs when applications initiate obscured information flows without the user's initiation. The most invasive are trojan horses and remote administration tools. After a user unwittingly executes these programs, they permit a remote trojan user to control the user's computer. The remote trojan user's access to information on the computer is coextensive with the user's. The most prominent examples of this kind of application are Back Orifice and Back Orifice 2000.<sup>[84]</sup>

The legitimacy of these programs exists on a continuum. Back Orifice's publisher's claims that it functions as a free, open source replacement to commercial remote administration programs with better encryption. Although those claims are probably best viewed as sophistry, they are perfectly true.<sup>[85]</sup> The publishers of NetBus have successfully legitimized their product to the point that anti-virus programs will no longer prevent the installation of NetBus.<sup>[86]</sup> And the publishers of Back Orifice validly point out that accepted commercial remote administration tools will perform silent and remote

installations.<sup>[87]</sup>

Applications besides remote administration tools collect information for their publishers. These applications have been collectively referred to as "spyware." The most legally prominent of these applications is RealNetwork's RealAudio. In a class action lawsuit against RealNetworks, the plaintiffs alleged "trespass to privacy and property, claiming RealNetworks software products secretly allowed RealNetworks to access and intercept users' electronic communications without their knowledge or consent."<sup>[88]</sup> The essence of the allegations was that RealAudio made record of the files that users downloaded and relayed this information to RealNetworks without giving any indication to the users of what was happening. The class action suit has been stayed by enforcement of the mandatory arbitration clause in the End User License Agreement included in every copy of relevant software.<sup>[89]</sup> A later RealNetworks application, Download Demon, had a similar function but disclosed it in the EULA.<sup>[90]</sup> Another class action lawsuit against Amazon.com its subsidiary, Alexa, alleged violations of ECPA has survived attempts to prevent the lawsuit from going forward as class action.<sup>[91]</sup> The lawsuit's core allegations were that Alexa's plug-in software, which provided additional information about website providers, leaked browser' habits back to Alexa without notice and in violation of the privacy policies of Amazon.com and Alexa. The Federal Trade Commission has reportedly initiated an investigation.<sup>[92]</sup>

Similar allegations have been made about the software that accompanies CueCat, a bar code scanner. CueCat's software attached unique identifying numbers to barcode queries that were sent to the databases of CueCat's manufacturer and cross-referenced with extensive profiles filled out by users in order to activate the software.<sup>[93]</sup> This was done without informing users.<sup>[94]</sup> Other notorious examples include Arthur's Reading Race, a children's educational game by Mattel,<sup>[95]</sup> Netscape's AOL Smart Download and Qualcomm's free version of Eudora.<sup>[96]</sup> In fact, hundreds of applications use

technology that surreptitiously discloses user information.<sup>[97]</sup>

### C. FLOWS FROM COMMUNICATION BETWEEN COMPUTERS

Data sent to another computer on the Internet must typically pass through networks and computer systems that are not under the control of the originator or the recipient. While the data is out of the control of originator and recipient, owners of intermediate computers could copy all their traffic rather than simply forwarding it.

Increasingly, users operate behind firewalls that monitor and control their on-line behavior.<sup>[98]</sup> A survey conducted by the American Management Association revealed that 27% of employers store and review users email and 21.4% store and review files users have transmitted in 1999 (up from 20.2% and 19.6% respectively in 1998.)<sup>[99]</sup> There are a multiple of widely used commercial software products that permit corporate firewall managers to control and monitor employee's Internet activities.<sup>[100]</sup>

Governments also monitors network traffic in transit. Many government surveillance systems are installed by the government at the access provider's facilities or installed by the access provider under government order. The American, British and Russian surveillance systems are the most publicized. The U.S. Federal government implemented "Carnivore," a system designed to selectively monitor the activities of an individual user (and therefore compliant with ECPA).<sup>[101]</sup> The United Kingdom has passed the Regulation of Investigatory Powers Act of 2000 (RIP), which permits the Secretary of State to impose "such obligations as it appears to him [or her] reasonable to impose for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and compiled with."<sup>[102]</sup> The end result of RIP is a legal regime authorizing the UK government to install "black boxes" to Internet access providers "that can be switched on under warrant to pipe data to a unit in the building of MI5, Britain's internal intelligence service."<sup>[103]</sup>

The Russian Federation's Federal Security Service (FSB) promulgated an order on the System of Operational Research Actions (SORM-2) which required Internet access providers to install systems that could monitor their users.<sup>[104]</sup> The Russian Supreme Court recently ruled that the operation of SORM required warrants, evidently overturning some of the FSB's order.<sup>[105]</sup>

#### **D. REFERENCING THE FACTS**

In the next Section's discussion of how the metaphor of cyberspace could permit the law to provide predictable and just outcomes, this article will reference some of the information flows previously mentioned in this Section. This Section provides a basis for discussing the current state of the Internet. Rooted in language developed for previously discussed technology, the law is able to adapt to the current state of the Internet only roughly. The final Section will consider the remaining information flows to ensure the robustness of the metaphor.

#### **IV. APPLICATION OF THE METAPHOR**

This section makes three applications of the cyberspace metaphor. The metaphor provides the most practical utility in the context of trespass to chattels actions against unauthorized use of network resources. Endorsing the metaphor would permit the law to convert actions for trespass to chattels to actions for trespass on real property. Converting trespass to chattels actions to trespass on real property solves nagging damages issues that complicate straightforward application of the law to stop spammers and others from abusing network resources.

Second, the cyberspace metaphor provides a critical perspective on state and federal computer fraud laws. The word "access" has been adopted by most legislatures, but courts have sometimes struggled to fix boundary of liability at "access." Furthermore, the cyberspace metaphor can assign privacy and property right on the modern Internet much better than current computer fraud laws. "Access" terminology confounds the

consistent, practical and efficient application of current laws to modern information flows.

Finally, the cyberspace metaphor adds to the debate over the Digital Millennium Copyright Act, which reinforces "trusted systems." Although it is beyond the scope of this article to discuss on which side of the debate the public good lies, the metaphor permits a new examination of the issues involved.

## A. TRESPASS TO CHATTELS AND STRONG FENCES

### 1. BACKGROUND

*State v. McGraw*<sup>[106]</sup> first recognized that misappropriation of computer resources could constitute trespass against chattels.<sup>[107]</sup> In overturning a conviction for theft, McGraw found that the storage of data for an employee's outside business was more like trespass against chattels.<sup>[108]</sup>

The first actual application of the trespass to chattels tort to computers did not occur on the Internet but over a phone line. In *Thrifty-Tel, Inc. v. Bezenek*,<sup>[109]</sup> the defendant's underaged sons made long distance phone calls through the unauthorized use of Thrifty-Tel's long-distance telephone service.<sup>[110]</sup> Long-distance phone calls could be made without charge through the use of Thrifty-Tel's telephone service with an access code and an authorization code.<sup>[111]</sup> With an access code provided by a friend, Bezenek's sons used a computer and a modem to automate a random search for authorization codes.<sup>[112]</sup> Thrifty-Tel filed suit and the court acknowledged the defendant's liability for trespass to chattels.<sup>[113]</sup> Trespass to

chattels requires tangible interference with the property. The court was willing to find that the defendant's repeated phone calls constituted tangible interference, but it required an extension of the law.

The modern rule recognizes an indirect touching or entry: e.g., dust particles from a cement plant that migrate onto another's real and personal property may give rise to trespass. . . . But the requirement of a tangible has been relaxed almost to the point of being discarded. Thus some courts have held that microscopic particles . . . or smoke . . . may give rise to trespass. And the California Supreme Court has intimated migrating particles (e.g., sound waves) may result in a trespass, provided they do not simply impede an owner's use or enjoyment of property, but cause damage. . . . In our view, the electronic signals generated by the

[114]

Bezenek boys' activities were sufficiently tangible to support a trespass cause of action.

As Professor Dan Burk notes, however, the actions cited by *Thrifty-Tel* were actions for trespass to lands. [115] Burk objects that trespass to chattels does not entail "the interest of inviolability that attends trespass to lands," and that even within "the context of real property, impinging ephemeral substances . . . or intangibles . . . typically have been addressed by doctrines of nuisances [116] rather than doctrines of trespass." [117] Burk also argues that trespass to chattels is a deficient legal theory in this context because it requires that some actual harm or impairment must be shown; either the owner is dispossessed of his property, the quality or condition of the property is impaired, the owner is deprived of the use of the property for a substantial time or some bodily harm is caused. [118]

## 2. ADOPTION AND DEVELOPMENT

Despite these flaws, courts have widely adopted the trespass to chattels theory in lawsuits by email providers against spammers. [119] Courts found two common, relevant elements in these cases; first, by consuming system resources, spam impaired the condition of the email servers (namely, by consuming computer resources and generating complaints from subscribers) and, second, defendants received some sort of notice that their use was unauthorized (either explicit written notice or notice in a Acceptable Use Policy.) [120] In *CompuServe Inc. v. Cyber Promotions, Inc.*, the

defendants raised the issue of implied consent.<sup>[121]</sup> The court acknowledged that "there [was] at least a tacit invitation for anyone on the Internet to utilize [CompuServe's] computer equipment to send e-mail to its subscribers" because of the utility CompuServe derived from having its subscribers receive email.<sup>[122]</sup> The court found the defendants' claims that this invitation could not be revoked (and therefore neither could the implicit consent) "erroneous under Ohio law."<sup>[123]</sup> This line of cases never found that the spam caused the computer to actually reach maximum capacity, possibly because impairment could always be found in subscriber complaints. It was therefore not necessary to turn to computer resource consumption to find impairment.

The trespass to chattels theory has spread to other contexts on the Internet. In *eBay, Inc. v. Bidder's Edge, Inc.*,<sup>[124]</sup> the court found that the automated retrieval of eBay's web pages and consequent indexing of eBay auctions by a Bidder's Edge program constituted trespass to chattels.<sup>[125]</sup> *eBay, Inc.* explicitly addressed the impact of unauthorized consumption of computer resources where the consumption did not cause the computer to reach maximum capacity.<sup>[126]</sup> The court's findings seem to impute the inviolability of chattels by conflating the absence of a right for Bidder's Edge to use eBay's property with eBay's legal right to exclude Bidder's Edge.<sup>[127]</sup> *Register.com, Inc. v. Verio, Inc.* used the same standard of harm to impose liability for trespass to chattels on Verio, where Verio accessed Register.com's public WHOIS database for marketing purposes.<sup>[128]</sup>

### 3. A TRESPASS TOO FAR?

Burk makes two *reductio ad absurdum* arguments against the application of trespass against chattels. First, he raises the possibility of extending the trespass to chattels theory to other contexts.

One wonders where the limits of such 'trespass by electrons' might lie. If one is willing to

base the physical contact requirement of trespass upon the receipt of electrons, then whole new vistas of electronic trespass are opened to our view. Unwanted telephone callers would seem to be engaging in trespass to chattels; the telephone call sends signals to the instrument of the recipient. So, too, with fax machines that receive unwelcome transmissions.

[129]

This result is not so absurd, however. Federal law already gives telephone and fax owners certain private rights of action against certain unsolicited commercial callers.

[130] Some of those prohibitions protect the same interests at stake in these cases; interlopers should not be able to impair the value or impose extra costs on the owner of communications equipment. Secondly, Burk argues that the computers cannot legally be considered to be harmed if they function as they were designed to do (that is, email servers are not harmed by sending email.) [131] This argument does not recognize the rights of owners that underlie the legal theory of trespass to chattels. A similar argument could be made about joyriding in a car. The joyrider's use of the car causes no harm to the car, but is unauthorized. Nevertheless, it is not controversial that depriving the car's owner the use of the car is a valid basis for liability, no matter that no harm was caused to the car.

But Burk's last policy argument presents a much more potent objection to the theory of trespass to chattels. Burk cites *Intel Corp. v. Hamidi*, [132] where Intel sued a former employee who sent email critical of Intel to Intel employees through Intel's own email servers. The court found that a connection to the Internet did not transform the email servers from private property to a "public forum," where Hamidi would be immune from legal intervention by the property owner. Hence, the court rejected Hamidi's First Amendment defenses. Burk argues that the application of the theory trespass to chattels to the Internet could have severe effects on the function of the Internet as a whole. [133] *Hamidi* stands as an example of how trespass to chattels can be used as an arbitrary barrier on the Internet. Burk argues that exercise of property rights in an environment like the Internet represents a threat to the functionality of the system as a whole.

[P]roprietization in a networked environment encourages the holder of the exclusive right to attempt to free-ride upon the external benefits of the network, while at-will avoiding contribution of such benefits to others. For example, in the *Hamidi* case, Intel apparently wished to enjoy the advantages of e-mail access to the Internet from its system, which was the reason it connected its machinery physically to the network. At the same time, it hoped to make its system unavailable to Hamidi, at least for the transmission of content that the company found objectionable. . . . Intel or eBay may hope to avoid the local burden of networking by legal exclusion, but this eventually will result in suppression of the positive externalities of networking. . . . If proprietization via trespass imposes costs in excess of the costs imposed by spam, it is difficult to justify recognition of trespass claims: they may do more harm to the digital commons than do the unauthorized uses they are designed to

[\[134\]](#)  
prevent.

Users would need to seek the permission of each individual computer owner their traffic passed over if trespass to chattels was taken to its extreme. Burk's argument is potent because it addresses how the exercise of property rights could effectively destroy the public nature of the Internet. Nevertheless, two answers to it can be raised.

First, computer owners are capable of employing technical measures to prevent many unauthorized activities that might otherwise contribute to the commons of the Internet. Eliminating the tort of trespass to chattels from the law applicable to the Internet would not save the Internet commons from privatization. Moreover, legal rules prohibiting such technical measures seem like a dramatic curtailment of property rights.

Second, Burk's economic analysis is specific to spam. Other activities with different economic effects need to be regulated. Application of the trespass to chattels theory might be inefficient with respect to spam but efficient with respect to hacking, spyware or cookie placement. Moreover, property rights are based in personal autonomy, not economic efficiency; we cannot include spam under trespass to chattels and then exclude Hamidi's messages, without implicating the coherence of the law. As previously argued, the incoherence and unpredictability of the law have their own economic costs. Ultimately, inconsistent legal rules are more inefficient than permitting proprietization of the Internet when technical measures can impose the same loss of open access in any

event.

#### 4. APPLICATION OF THE METAPHOR: THE IMPORTANCE OF FENCES

As a strict matter of law, Burk's contention that trespass to chattels does not technically cover spam or unauthorized indexing may be correct.<sup>[135]</sup> (I equivocate because the courts have established all the elements of trespass to chattels to their own satisfaction and the courts' definition is self-reinforcing in a way Burk's analysis is not.) Indeed, Susan Ballantine contends that courts should analogize and use trespass on lands precisely because trespass to chattels is inadequate for the situation.<sup>[136]</sup> Using the cyberspace metaphor provides an easy exit to this dilemma. If we envision email servers as a physical space, then spam is easily perceived as a nuisance. The cyberspace metaphor transforms trespass to chattels to trespass on real property.

The application of the metaphor of fences in cyberspace requires us to examine the plaintiff's technical measures to prevent the defendants from consuming their computer resources. The rule of fences holds that the law will not fix liability unless the defendant circumvents reasonable technical measures implemented by the plaintiff. In fact, most of the spam cases mention defendants' measures to conceal the origin of their messages.

*CompuServe* discussed the legal right of chattel owners to take such measures.<sup>[137]</sup>

*Bidder's Edge, Inc.* discussed the extensive measures eBay took to prevent Bidder's Edge indexing eBay.<sup>[138]</sup> The only case previously cited which does not discuss technical measures to prevent defendants' actions is *Hotmail Corp. v. Van\$ Money Pie*, where the defendants used accounts at the plaintiff's free email service to send spam.

<sup>[139]</sup> Given that Hotmail offered free email accounts to the general public, the costs of screening may have been unreasonable. It may be that there were no possible technical measures to be taken in *Van\$ Money Pie*. In these cases, the "fences in cyberspace" analysis looks to see whether reasonable technical measures were available and whether the technical measures taken were reasonable.

The benefits of the analysis associated with the application of the metaphor are threefold. First, the metaphor eliminates the technical problem in the law described by Burk and Ballantine. Second, the metaphor promotes technical solutions. Consider that if the technical measures taken in the above cases were found to be inadequate, more effective technical measures would have to be used. Technical measures are preferable to judicial action: the *CompuServe* court noted that "the implementation of technological means of self-help, to the extent that reasonable measures are effective, is particularly appropriate in this type of situation and should be exhausted before legal action is proper."<sup>[140]</sup> Users would benefit more from technical measures against spam that worked universally than from a legal remedy that applied to a limited set of defendants and whose enforceability was not reliable. Finally, fences promote free space and open access on the Internet. Burk's root concern is the erosion of common land in cyberspace. Under the cyberspace fences metaphor, computer owners who do not choose to erect fences have no basis to assign liability to users who consume their property. While the law should not prevent the erection of fences on private land, it can assume that whatever is not fenced off is free to use. The assumption behind open access resembles the legal rule articulated in *Buford v. Huotz*,<sup>[141]</sup> which promoted free use of unenclosed portions of the Western range because such use benefited agriculture, the economy and ultimately, society.<sup>[142]</sup>

## **B. COMPUTER FRAUD, ACCESS AND NMAP**

### **1. ACCESS AS THE THRESHOLD OF LIABILITY**

Most American jurisdictions have computer crime laws which include prohibitions on unauthorized access. Seven states are exceptions. Georgia, Montana and Virginia criminalize unauthorized use of a computer.<sup>[143]</sup> Minnesota criminalizes the "penetration" of a computer or computer system.<sup>[144]</sup> Wisconsin criminalizes the access of data, computer programs and documentation, but requires that computer equipment itself be modified, damaged or destroyed.<sup>[145]</sup> (Section IV.B.2 discusses the remaining

states, New York and Massachusetts, separately.) Of the remaining forty-three states, only Alaska, Louisiana, Michigan, Mississippi, South Carolina, and West Virginia require some other element beyond unauthorized access and *mens rea* (typically including modification or destruction of data or fraud.)<sup>[146]</sup> Thirty-seven other states require only access and *mens rea*.<sup>[147]</sup> As a threshold for criminal liability, "access" proves to be a tremendously porous border. Statutory definitions of access are remarkably homogeneous and quite broad. The table below shows how twenty one states use essentially three definitions for access.

### POPULAR STATE DEFINITIONS OF ACCESS

Alabama, Arkansas, Connecticut, Delaware, Iowa, Kansas, and New Hampshire statutes. <sup>[148]</sup>	Arizona, Florida, Kentucky, Indiana, North Dakota, Ohio, Oregon, Texas and Wyoming statutes. <sup>[149]</sup>	Idaho, Missouri, Nebraska, New Jersey and Vermont statutes. <sup>[150]</sup>
"to instruct, communicate with, store data in, or retrieve data from a computer, computer system or computer network"	"to approach, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network"	"to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system, or computer network"

Another thirteen states use very similar definitions to those presented in the table.<sup>[151]</sup> (California, Maine, Hawaii and Oklahoma) define access as "entry" into a computer system.<sup>[152]</sup> The federal computer fraud statute (Computer Fraud and Abuse Act) protects only limited class of computers; the most broadly-defined category of computers are those involved in interstate or international communication.<sup>[153]</sup> The CFAA criminalizes intentionally accessing and obtaining unauthorized information from a

computer across state or national boundaries.<sup>[154]</sup> The federal computer fraud law does not define access.<sup>[155]</sup>

## 2. DEVELOPMENTS LIMITING APPLICATION OF COMPUTER FRAUD LAWS

The homogeneity may be evidence of legislative inexperience rather than a well-tested regime for criminal liability.<sup>[156]</sup> Viewing warning banners and password prompts by unauthorized users constitutes communicating with a computer and receiving data from computers. As such, those activities would fall under a stringent interpretation of most definitions of access and would trigger liability. Such an interpretation would not provide users with notice that a use is unauthorized. Interaction with any computer connected to the Internet satisfies most statutory definitions of "access." The boundary of liability falls back to the authorization or consent of the computer owner. *Register.com, Inc. v. Verio, Inc.* provides one unsettling example of how easily liability can be incurred.<sup>[157]</sup>

Addressing Register.com's CFAA claims based on Verio's access to Register.com's public WHOIS database, the court notes simply "because Register.com objects to Verio's use of search robots they represent an unauthorized access to the WHOIS

database."<sup>[158]</sup> Although the court did base Verio's liability for trespass to Register.com's chattels on the Verio's notice that its access of the WHOIS database was

unauthorized, it is unclear whether the court also based the CFAA claim on notice.<sup>[159]</sup> In any event, because liability expands and contracts at will, the threat of liability could hinder interactions on the Internet. Moreover, computer owners have no incentive to implement technical measures to exclude others. Technical measures would function more efficiently than judicially imposed sanctions, if only because they do not involve the same chill on interactions with the Internet.

The overexpansiveness of these laws has contributed to the unpredictability of their application; courts are resistant to interpreting statutes' full potential scope. For example, in *State v. Rowell*, the New Mexico Supreme Court found that the New Mexico computer

fraud statute could not be applied a defendant who defrauded his victims over the telephone.<sup>[160]</sup> The court found that the fraudulent calls were made through "computerized switches" and that the defendant's action's "resulted in the access of computerized switches, and in fact access to a computer or a computer network."<sup>[161]</sup> Nevertheless, the court concluded that the "access of such components is not the type of conduct the legislature sought to punish by the Act."<sup>[162]</sup> Furthermore, in *State v. Allen*, the Kansas Supreme Court substituted a dictionary's definition of "access" in place of the "tortured translation of the definition . . . provided" by the Kansas computer fraud statute, rather than hold the statute unconstitutionally vague.<sup>[163]</sup> This interpretation favored the defendant, where the defendant had called a Southwestern Bell computer but where there was no evidence that the defendant had attempted to respond to the password prompt.<sup>[164]</sup> At the same time, the court resisted the state's argument that Southwestern Bell's investigative costs were the measure of the defendant's damage to Southwestern Bell's computer system. The court commented that "a fitting analogy [is] that the State is essentially saying that a person looking at a no trespassing sign on a gate causes damage to the owner of the gate if the owner decides as a result to add a new lock."<sup>[165]</sup> In *Moulton v. VC3*, a federal court found that the costs incurred investigating a port scan did not constitute damages under the federal Computer Fraud and Abuse Act.<sup>[166]</sup> Moreover, the court found that a party's port scan did not access the other party's network.<sup>[167]</sup> Port scans elicit information from computers and computer networks; under many of the state statutory definitions above, port scans do access computers and probably would constitute computer crime. Certainly, the court could have found port scans to constitute access under the CFAA and found the party liable for the port scan. *Moulton* may signify that there is a threshold of network activity below which courts will not interfere.<sup>[168]</sup>

However, not all state statutes provide for such expansive liability. A small minority of states, Connecticut, Ohio, New Hampshire and West Virginia, provide affirmative

defenses to offset the expansiveness inherent in "access" when defendants reasonably believed that they were authorized or could not have known they were unauthorized.

[169] Massachusetts criminalizes knowing, unauthorized access and failure to terminate access after becoming aware that access is unauthorized. [170] Moreover, the Massachusetts statute states that the requirement of a password constitutes notice that access is limited to authorized users. [171] Massachusetts has made some provision to limit liability and, more importantly, given a concrete guide to the limits of access. New York, on the other hand, criminalizes only unauthorized use where "the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system." [172] This qualification was held to limit liability in *People v. Angeles*, where a defendant obtained and sold a copy of the Empire Car Service's customer list and the prosecution failed to allege that Empire Car Service's computer system had any sort of computer security system. [173] Instead the court noted that

The legislative history of the statute makes clear that this requirement was included on the ground that "[s]uch protective devices provide the first line of defense against unauthorized intrusion into a computer system." . . . The Legislature thus put computer owners on notice that in order to receive the protection of the criminal statute, they must equip their computers with some kind of protection mechanism, such as a password requirement or a lock. [174]

While password prompts and warning banners may lie just beyond a common-sense threshold of access, there are many times where computer crime occurs without encountering a password prompt. Moreover, there may be situations where consideration limited to password prompts will not adequately analysis the entire bundle of rights inherent in computer property connected to the Internet.

### **3. TRANSLATING "ACCESS" INTO REAL LIFE ON THE INTERNET**

The application of access-based computer crime laws could damage the digital commons as much as the current formulation of trespass on chattels. The efficiency of

communication on the Internet stems from the implied consent to use the computer resources and information of others'. Legal rules that extend liability to any access whatsoever damage that efficiency. Consider how trespass to chattels and access-based computer crime laws would function on the Internet. These laws implicate the most rudimentary network functions, like pinging an IP address to see if a network host is connected to the Internet, let alone initiating a TCP connection that would provide the basis for communicating that access is unauthorized.

The benefit of the fences in cyberspace metaphor is an enhanced capacity for precision. Application of the metaphor of fences in cyberspace could create a legal regime capable of much finer distinctions between liability and non-liability. Consider a situation where the law assigns a privacy right to the computer owner over the kind of operating system running on the computer. (This privacy right is, and should remain, a hypothetical situation. The overall utility of such a privacy right is questionable. While discovering the identity of a target's operating system is an integral step to breaking into the target, it is poor security to rely on the obscurity of the operating system's identity.)<sup>[175]</sup> In cyberspace, information about the kind of operating system is an object. This hypothetical posits that the owner has the legal right to put a fence around this object. Individuals on the network can use techniques like banner grabbing, port scanning or nmap's OS fingerprinting to identify the owner's operating system.<sup>[176]</sup> Most "fences" would protect against banner-grabbing; banners must be either changed or eliminated.<sup>[177]</sup> Port scanning can be prevented by shutting down unnecessary applications and through using firewalls that filtered packets on the basis of port numbers.<sup>[178]</sup> These measures would create a fences that encompasses more of the information. Finally, preventing nmap-type OS fingerprinting requires using a firewall that filtered on a packet-by-packet basis or altering the TCP/IP stack of the computer.<sup>[179]</sup> These measures would enclose most of the remotely available information about a computer's operating system. A court deciding whether to assign liability would first inquire into what technical measures were used; the court must find the fences in cyberspace. Next, the court must decide whether the technical measures were reasonable. The computer owner who

failed to protect against banner-grabbing should not have legal recourse when banner grabbing identifies his operating system. A computer owner who used a firewall that prevented port scans but not nmap-type OS fingerprinting might establish a strong case for liability against a nmap scanner. Then again, perhaps the cost of preventing nmap-type OS fingerprinting might be found minimal; the court might assign liability only where the defendant used other means to get the information. The point of the exercise above is that the metaphor allows courts to distinguish between relative degrees of care that the owner has taken to restrict information flows.

Courts striving for equitable and predictable distinctions between liability and non-liability receive little help from the language of the law; most current laws could be used to penalize any interactions on the Internet between networked computers. To be efficient, the law must also be capable of precision and coherency, even more so because information flows on the Internet can be very complex. The cyberspace fences metaphor can help provide that precision.

## **C. "TRUSTED SYSTEMS" AND CONFLICTED PROPERTY RULES**

### **1. FROM "TRUSTED SYSTEMS" TO THE LAW**

Software creates "trusted system" by disabling some of the usual capabilities of the computers on which it is run.<sup>[180]</sup> "Trusted systems" are granted some privileges in return for accepting the limitations placed on them. Increasingly, software publishers are turning to "trusted system" technology to enforce agreements with software users.<sup>[181]</sup> Mostly, software publishers use "trusted system" technology because of their concern that their copyrights would otherwise be violated by users copying and distributing an infinite number of perfect digital copies.<sup>[182]</sup> "Trusted system" technology is used to prevent users from copying and distributing copyright owners' works.<sup>[183]</sup> In this context, "trusted system" technology is also called rights management systems.<sup>[184]</sup> "Trusted system" technology is also used to ensure that the players of Internet-based

games to not use illicit technology to cheat.<sup>[185]</sup> The client/user side of "trusted system" technology is very vulnerable, because users are free to study methods of attacking the technology at their leisure. Commentary on the seemingly innocuous example of Internet games shows how difficult it is to implement effective "trusted system" technology.<sup>[186]</sup> The most salient example of client side attacks on rights management system is the failure of the Secure Digital Music Initiative standard.<sup>[187]</sup> The vulnerability of the client side of "trusted systems" technology has led one computer security authority, Bruce Schneier, to declare: "there is no way to trust a client-side program in real usage" and that, in fact, it is not possible to implement effective "trusted system" technology.<sup>[188]</sup>

Recognition of the inherent vulnerability of "trusted system" technology led to the Digital Millennium Copyright Act.<sup>[189]</sup> The DMCA prohibits the circumvention of technological measures that effectively control access to copyright owner's work, as well as the manufacture and distribution of technologies of devices whose principle purpose is such circumvention.<sup>[190]</sup> The DMCA also prohibits the manufacture or distribution of devices or technologies that circumvent technological measures that effectively protect the rights of copyright owners.<sup>[191]</sup> The DMCA provides exceptions for nonprofit libraries, educational institutions and archives,<sup>[192]</sup> law enforcement activities,<sup>[193]</sup> reverse engineering,<sup>[194]</sup> encryption<sup>[195]</sup> and security research<sup>[196]</sup> and the protection of personally identifying information.<sup>[197]</sup> Violations of the DMCA are punishable civilly<sup>[198]</sup> and criminally.<sup>[199]</sup>

Many criticisms of the DMCA focus on the DMCA's failure to accommodate fair use. Fair use is a defense against a claim of a copyright holder for copyright infringement.<sup>[200]</sup> Fair use encompasses traditional prerogatives of copyright users,<sup>[201]</sup> including First Amendment rights to free speech.<sup>[202]</sup> "Trusted systems" are not required to

incorporate fair use exemptions into their functionality, but circumventing "trusted system" technology for fair uses still results in civil and criminal penalties under the DMCA.<sup>[203]</sup> This concern with the DMCA was borne out by the Copyright Office's exemptions for encrypted lists of websites blocked by filtering software applications and literary works (including computer programs) protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence.<sup>[204]</sup> The Copyright Office made explicit statements about the fair use values that necessitated the filtering software exemption:

[R]eproduction or display of the lists for the purpose of criticizing them could constitute fair use. . . . [A] persuasive case was made that the existence of access control measures has had an adverse effect on criticism and comment, and most likely news reporting, and that the prohibition on circumvention of access control measures will have an adverse effect. Thus, it appears that the prohibition on circumvention of technological measures that control access to these lists of blocked sites will cause an adverse effect on noninfringing users since persons who wish to criticize and comment on them cannot ascertain which sites are

<sup>[205]</sup>  
contained in the lists unless they circumvent.

The Copyright Office also made reference to the First Amendment issues implicit in the public dissemination and discussion of the sites blocked by filtering software, especially where adults using public libraries might not be able to receive speech because of the filtering software.<sup>[206]</sup>

## 2. APPLICATION OF THE METAPHOR

The DMCA fits well into the language of the metaphor. Copyrighted works are a property in real life and in cyberspace; access to that property is controlled by technological fences. After satisfying the license requirements for access, a user is permitted access, but the ability to copy and distribute data in his own computer is fenced off. Although the work is on the computer owner's cyberspace, he or she is not able to control it. The DMCA's threshold of liability coincides precisely with the metaphors. Circumvention of technical measures are jumping over fences in cyberspace are equivalent and prohibited.

In this way, the DMCA creates consistent and coherent rules and provides copyright owners' strong incentives to use technical measures before turning to courts. *Universal City Studios, Inc. v. Reimerdes*, the first application of the DMCA, found the application of the law "clear," and that there was "no serious question" that the defendant's behavior violated the statutory provisions in the DMCA.<sup>[207]</sup>

### 3. WHOSE PROPERTY RIGHTS TRUMPS?

Although the DMCA coincides precisely with the metaphor, the significance of the metaphor to critical analysis of the DMCA merits more than a perfunctory discussion. The DMCA controversy raises the issue what residual property rights of computer owners remain after using copyrighted software with DMCA-protected technical measures. This question is more complicated than identifying computer owner's *a priori* property rights. How should the law permit software to curtail computer owners' property rights who knowingly and willingly run the software? This question encompasses issues with obvious answers, like virii and trojan horses. It also encompasses more ambiguous matters. Lawsuits have been filed against against software publishers whose software gathered information about users without explicitly saying so<sup>[208]</sup> and against America Online, whose software made it difficult to revert to competing Internet access providers and web browsers after installation.<sup>[209]</sup> The merit of these lawsuits may well hinge on the availability of technical measures that would have prevented or reversed the harm at issue. Analyzing those lawsuits from the perspective of the fences in cyberspace metaphor, the liability of the defendants depends on whether they circumvented technical measures implemented by the computer owner. The transfer of cookies can be prevented by proper configuration of the browser, while the configuration of Internet connectivity software may be substantially more complicated and controlling the effects of installed software is extremely difficult. Preventing or reversing the harm caused by America Online is much more difficult for most consumers than preventing the harm caused by Internet advertisers using cookies.

For computer owners to enjoy their property rights, implementation of technical measures that control software will be increasingly needed. The problem is that technical measures employed by computer owners will conflict with technical measures implemented by software publishers. Technical measures implemented by the computer owner protect and control his property, while technical measures implemented by copyright owners provide control over their work at the expense of the computer owner. One easily analogized example of a brewing technological conflict between consumers and website operators over banner ads and cookies. Many website operators employ banner ads to subsidize their operations. At the same time, users resentful of the privacy implications employ software that manipulates cookies and prevents banner ads from loading.<sup>[210]</sup> Reacting to this software, some web site operators use technical countermeasures to prevent browsers that won't load ads from loading at all.<sup>[211]</sup> Others have responded with threats to boycott or to sue the publishers of this software, under the theory that use of the software violated the web site operators' copyright.<sup>[212]</sup> This technological struggle does not beg the question of whether the consumer or the web site operator have property rights in their respective computers and the information on them. They should both retain rights in their property. Instead, this struggle begs the question of who has yielded those rights. Has the consumer yielded his property rights over his computer by loading a web page and is he now required to display the page however web site operator wishes? Or has the web site operator yielded his right to control his data by making the web page publicly accessible over the Internet? Returning to DMCA considerations, to the extent that property rights can and should coincide with effective technical measures protecting property, whose rights should dominate, computer owners or copyright owners?

Arguments against the DMCA have not yet considered the effect of the DMCA on the property of computer owners. Although it may be effectively countered by theories of implied or explicit consent, this argument at least addresses the loss of functionality and property rights computer owners must accommodate to avoid liability under the DMCA.

## V. CONCLUSION

The fences in cyberspace analysis addresses shortcomings in modern law. Certainly, the metaphor trims back overexpansive doctrines of trespass on chattels and statutory computer crimes. The metaphor also describes the controversy over the DMCA in terms of property rights, instead of fair use and copyright. But the fences in cyberspace metaphor provides for a more precise and coherent line between property rights, the DMCA discussion shows that it does not address the underlying allocation of property rights. The analysis provided by the metaphor comes full circle, hopefully with a clearer conception of the practical values involved.

---

[1] Equity is defined as "[j]ustice administered according to fairness [rather than according to the letter of the law]." BLACK'S LAW DICTIONARY 540 (6th ed. 1990).

[2] A license is defined as "[a] personal privilege to do some particular act or series of acts on land without possessing any [property] interest therein, and is ordinarily revocable at the will of the licensor [that is, the landowner], and is not assignable [that is, transferable to someone else.]" *Id.*, at 919. An implied license is "one that presumed to have been given from the acts of the party authorized to give it." *Id.*, at 920.

[3] In *Reno v. ACLU*, 521 U.S. 844, 849-50 (1997), the Supreme Court described the Internet as "an international network of interconnected computers . . . a unique and wholly new medium of human communication."

[4] Abstraction is defined as the "formation of an idea apart from concrete things, situations, etc." LEXICON PUBLICATIONS, WEBSTER'S DICTIONARY 4 (1987).

[5] Chattels are defined as "personal property, as distinguished from real property." BLACK'S LAW DICTIONARY, *supra* note 1, at 236. Trespass to chattels is defined as "unlawful and serious interference with the possessory rights of another to personal property. . . . [In contrast] every unauthorized and direct breach of the boundaries of another's land was an actionable trespass." *Id.* at 1503.

[6] *But see* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 5 (1999) (positing the first instances of the word cyberspace in the field of cybernetics, predating Gibson's publication).

[7] Cyberspace was described as a "consensual hallucination . . . a graphic representation of data abstracted from the banks of every computer in the human system. . . . [T]he interior of a given data construct possessed unlimited subjective dimension; a child's toy calculator . . . would have presented limitless gulfs of nothingness hung with a few basic commands." WILLIAM GIBSON, NEUROMANCER 51, 63 (1984). "In this fictional world of cyberspace, 'computer cowboys' neurologically patch themselves into computer networks where matrices of electronic data become cerebral manifestations. Without keyboards or data, cowboys navigate through data of individuals, firms and

governments as if the cowboys were suspended in a surreal fourth dimension." Michael P. Diercks, *Computer Network Abuse*, 6 HARV. J. LAW & TECH. 307, 307 n. 1 (1993).

[8]

A lot of silly stuff came out of [the genre which William Gibson pioneered.] Beforehand, when you were on the Internet you were merely slouched out in a chair, typing onto a CompuServe message board or something. Afterwards, you were flying bodilessly through cyberspace, a creature of pure data, communing with other cyberbeings through virtual reality. It's taken years to get people to stop talking that way, not to mention believing some of that bunkum.

Gavin McNett, *The Ambivalent Cyberpunk* at <http://www.salon.com/books/feature/2000/10/30/sterling/index.html> (Oct. 30, 2000).

[9] See LESSIG, *supra* note 6.

[10] *Id.*, at 26.

[11] *See id.*

[12] *See id.*

[13] *See id.*, at 63-84 (describing how the various architectures of America Online, Counsel Connect, an NYU multi-user dungeon (MUD), and a law school email list permitted different types of control and embodied different types of values).

[14] *See, e.g.*, Michael Johns, Comment, *The First Amendment and Cyberspace: Trying to Teach Old Doctrines New Tricks*, 64 U. CIN. L. REV. 1383 (1996); Harold Reeves Smith, Comment, *Property in Cyberspace*, 63. U. CHI. L. REV. 761 (1996).

[15] *See, generally*, Stephen J. Saphranek, *Can Science Guide Legal Argumentation? The Role of Metaphor in Constitutional Cases*, 25 LOY. U. CHI. L.J. 357, 358 (1994); *see also id.*, at 358 nn. 9-10; A. Michael Fromkin, *The Metaphor Is Key: Cryptography, The Clipper Chip and the Constitution*, 143 U. PA. L. REV. 709, 859-62 (1995).

[16] *See, e.g.*, *Bd. Of Educ. v. Allen*, 326 U.S. 236 (1968); *Everson v. Bd. of Educ.*, 330 U.S. 1 (1947); *Reynolds v. United States*, 98 U.S. 145, 165 (1878); Diercks, *supra* note 7.

[17] *See, e.g.*, *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 US 419, 435 (1982); *Kaiser Aetna v. United States*, 444 U.S. 164 (1979).

[18] *See* Saphranek, *supra* note 15, at 401-02 (appraising "bundle of rights" metaphor as generally successful).

[19] *See id.*, at 398 (discussing the failure of the wall metaphor); *see also id.*, at 372 n. 80 (citing *Allegheny County v. Greater Pittsburgh ALCU*, 492 USC 593 (1989); *Wallace v. Jaffree*, 472 US 38 (1985); *Committee for Pub. Educ. and Religious Liberty v. Regan*, 444 US 646 (1980) as cases where the Supreme Court has directly or indirectly disclaimed reliance on the wall metaphor).

[20] "The essence of private property is always the right to exclude others." MORRIS R. COHEN, LAW AND THE

SOCIAL ORDER 46 (1967). *See also Loretto*, 458 US at 435 ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights").

[21] *See Smith, supra* note 14, at 778.

[22]

To date, the battles for system security and user privacy have been fought almost entirely at the system level. [Smith uses the system level as shorthand to refer to a network bordered by a firewall and controlled by a system administrator.] The system administrator, charged with constructing and maintaining the system-level firewall, is in the best position to protect security and privacy through the use of that firewall. The firewall prevents infiltration not only by shielding it from viruses spreading across the Internet but also by shutting out hackers set on either sabotaging the system or accessing individual files and e-mail records. [T]he system administrator is more likely than the individual users of his system to possess the technical expertise needed to protect security and privacy effectively.

*Id.* at 770 (citations omitted). It is worth pointing out that the firewall may be the first line of defense against computer security violations, but it cannot be the only component in a comprehensive, effective security regime. *See Stephen Reed, Beyond Firewalls*, PC WORLD, August, 2000, at 46.

[23] *See Sophos, W32/Apology-B* at <http://www.sophos.com/virusinfo/analyses/w32apologyb.html> (last viewed Mar. 11, 2001).

[24] "The computer is a piece of tangible personal property." *Ticketmaster, Corp. v. Tickets.com, Inc.*, No. CV99-7954-HLH, 2000 U.S. Dist. LEXIS 12987, at \*15 (C.D. Ca. Aug. 10, 2000).

[25] *See* Section IV.A, *infra*; *see also IBM v. Comdisco, Inc.*, C.A. No. 91-C-07-199, 1991 Del. Super LEXIS 453 (Del. 1991).

[26] *See, e.g., State v. McGraw*, 480 N.E.2d 552, 554 (Ind. 1985) (use of city computers by city employee for outside business purposes that did not cause the computers to reach capacity and therefore did not deprive the city of anything of value did not constitute theft but could constitute trespass to chattels); *Evans v. Commonwealth*, 308 S. E.2d 126 (Va. 1983) (noting that VA. CODE ANN. § 18.2-98.1 (1978) effectively reversed the result in *Lund v. Virginia*, 232 S.E.2d 745 (Va. 1977), which found that the use of processing time was not theft).

[27] *See ProcessTree, How It Works* at <http://www.processtree.com/how.asp> (last viewed Nov. 19, 2000). Additionally, at least one American company is willing to provide "free" Internet service in exchange for otherwise unused processor power. *See Cryptome, Juno Apes Cops and NSSG in Asymmetrical Padwad* at <http://cryptome.org/juno-puke2.htm> (Feb. 3, 2001).

[28] *Engblom v. Carey*, 677 F.2d 957 (2d Cir. 1982) characterized itself as the first non-trivial federal consideration of the Third Amendment and the sole case finding a violation of the Third Amendment. *See id.*, at 959 n. 1.

[29] "No Soldier shall, in time of peace be quartered in any home, without consent of the Owner, nor in time of war, but in a manner to be proscribed by law." U.S. CONST. amend. III.

[30] *Engblom*, 677 F.2d at 962 (finding Third Amendment violation when National Guard first evicted striking state

prison guards then stationed themselves in the guards' dormitories).

[31] *See Rakas v. Illinois*, 439 U.S. 128 (1978).

Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. One of the main rights attaching to property is the right to exclude others . . . and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.

*Id.*, at 144.

[32] There are at least 157 law review articles on Internet privacy and 867 articles which mention that theme. Search of Lexis Combined Law Review Database, Lexis-Reed Elsevier (Nov. 19, 2000) (searches for articles containing "Internet" and "privacy" in the same in sentence in the summary field and anywhere in text, respectively).

[33] There is a difference between autonomous and willing disclosures. Autonomous disclosures are the result of the discloser's intentional actions. To contrast, a person coerced into disclosing financial data by the necessity of acquiring a bank account, driver's license or a telephone number has done so autonomously, but might argue that he or she has not done so willingly.

[34] *See, e.g.*, Privacy Act, 5 U.S.C. § 552a (2000) (limiting disclosure of information about citizens by federal agencies); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2000) (limiting disclosure of information about students by educational institutions); Right to Financial Privacy Act, 29 U.S.C. §§ 3401-22 (2000) (limiting disclosure of information about customers by depository institutions to federal law enforcement officials); Cable Communication Policy Act, 47 U.S.C. § 551 (2000) (limiting the disclosure of information about subscribers by cable companies); Video Privacy Protection Act, 18 U.S.C. § 2710 (2000) (limiting the disclosure of information about video renters by video rental stores); Drivers Privacy Protection Act, 18 U.S.C. §§ 2721-25 (2000) (limiting disclosure of information about drivers by state driver's licensing agencies); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06 (2000) (limiting collection and disclosure of information about children under 13 by website operators).

[35] 18 U.S.C. §§ 2510-22, 2701-09 (2000).

[36] Electronic communications are defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system." 18 U.S.C. § 2510 (12) (2000).

[37] *See* 18 U.S.C. § 2511 (2) (g) (2000).

[38] *See* 18 U.S.C. §§ 2511 (1) (a), (c), (d) (2000).

[39] *See* 18 U.S.C. § 2511 (1) (b) (2000).

[40] *See* 18 U.S.C. § 2512 (2000).

[41] *See* 18 U.S.C. § 2520 (2000).

[42] See 18 U.S.C. § 2701 (2000).

[43] See 18 U.S.C. §§ 2511 (2), (3), 2513, 2516-19, 2522, 2702 (b) (2), 2703-06, 2709 (2000).

[44] The Fifth Circuit has characterized the Wiretap Act as "famous (if not infamous) for its lack of clarity." *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994). The Ninth Circuit has stated that the Fifth Circuit "might have put the matter too mildly. Indeed, the intersection of the Wiretap Act and the Stored Communications Act is a complex, often convoluted, area of the law." *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998). Jerry Kang has described ECPA as "grossly complicated." Jerry Kang, *Information Privacy in Cyberspace Transaction*, 50 STAN. L. REV. 1193, 1233 (1998).

[45] See 18 U.S.C. §§ 1831-39 (2000).

[46] See 18 U.S.C. §§ 1831-32 (2000).

[47] 18 U.S.C. § 1839 (3) (2000).

[48] 236 F.3d 1035 (9th Cir. 2001).

[49] See *id.*, at 1041.

[50] See *id.*

[51] See *id.*, at 1046. Dicta suggests that anyone failing to conform the conditions accompanying access would also have run afoul of ECPA. See *id.*, at 1047.

[52] See *Smith*, *supra* note 14, at 766

[53] See *id.*

[54]

Computer time is a limited resource, and an operable computer that is unused or underused is a wasted resource. . . . [T]he law . . . must recognize . . . more permeable system boundaries become, the more those who need to will cross those boundaries and make use of those systems. Legal rules could, for example, encourage users to more efficiently allocate computer time, shifting operations from systems that are [overused] at certain hours to systems that are underused at those times. . . The same argument applies to the use of computer memory. A computer system with substantially more memory than its users require could be used to store information for others . . . Such an arrangement would facilitate information distribution without any serious impairment to the owner of the underused system.

*Id.*, at 787

[55] *Buford v. Hurotz*, 133 U.S. 320, 326-28 (1890); see also *id.*, at 330; *Kerwhaker v. Cleveland, Columbus and Cincinnati Rail Rd. Co.*, 3 Ohio St. 173, 179 (1854).

[56] See e.g., TIMOTHY PARKER, *TEACH YOURSELF TCP/IP IN 14 DAYS* Page 1-50 (2nd ed. 1996); Jason

Yanowitz, *Under the hood of the Internet: An overview of the TCP/IP Protocol Suite* at <http://info.acm.org/crossroads/xrds1-1/tcpjpy.html> (modified Jan. 20, 2000).

[57] See TIMOTHY PARKER, *supra* note 56, at 39-99.

[58] See Eric J. Sinrod & Williams P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 COMPUTER & HIGH TECH. L.J. 177, 190 (2000).

[59] See David Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3 ¶ 7 n. 12 (1999), at <http://www.jvolt.net/symp2000/johndoe.html> (citing Kang, *supra* note 44, 1225, 1233).

[60] WHOIS databases store information about who has the right to assign the individual IP addresses within a particular range. See, e.g., InternNIC, *Registry Whois Database* at <http://www.internic.org/whois.html> (last updated Oct. 26, 2000). Internet access providers provide this information to the Internet Assigned Numbers Authority's appointed regional internet registrars when the providers apply for IP ranges. There are three such registrars. In North America, South America, the Caribbean and sub-Saharan Africa, the American Registry of Internet Numbers assigns IP address ranges. See American Registry of Internet Numbers, *About ARIN* at <http://www.arin.net/arintro.html> (modified Sept. 15, 2000). This information includes points of contact (POCs) for the registrants. See American Registry of Internet Numbers, *ARIN: WHOIS* at <http://www.arin.net/arintro.html> (modified Sept. 11, 2000).

[61] See Sobel, *supra* note 59, at ¶ 7 n. 12

[62] See generally, *id.*

[63] See generally Kang, *supra* note 44, at 1242 n. 217.

[64] Securities Exchange Commission, *DoubleClick, Inv. 1998 10-K Form* at <http://www.sec.gov/Archives/edgar/data/1049480/0001047469-99-008506.txt> (Mar. 4, 1999).

[65] *In Re DoubleClick Inc. Privacy Litigation*, No. 1352, 2000 U.S. Dist. LEXIS 11148 (J.M.P.L. Jul. 7 31, 2000).

[66] See *In re DoubleClick Inc. Privacy Litigation*, No. 00 Civ. 0641 (NRB), 2001 U.S. Dist. LEXIS 3498 (S.D.N.Y. Mar. 28, 2001).

[67] See Lincoln Stein, *WWW Security FAQ: Client Side Security* at <http://www.span.org/doc/FAQs/cgi/wwwsf7.html> (modified Sept. 13, 1999).

[68] See *id.*

[69] See *id.*; Gary McGraw & Ed Felten, *Hostile Applets* at <http://www.cigital.com/javasecurity/applets.html> (last visited Nov. 25, 2000); Ed Kubatitis, *WWW Browser Security & Privacy Flaws* at <http://www.ews.uiuc.edu/~ejk/browser-security.html> (modified Jan. 11, 1999).

[70] See PrivacyTimes.com, *Not So Anonymous* at [http://www.privacytimes.com/NewWebstories/anon\\_priv\\_11\\_16.htm](http://www.privacytimes.com/NewWebstories/anon_priv_11_16.htm) (Nov. 4, 1999).

- [71] See David Brumley, *The Dangers of JavaScript* at <http://www.stanford.edu/~dbrumley/Me/javascript.htm> (Jan. 24, 1999).
- [72] See Gregori Guninski, *Internet Explorer security* at <http://www.guninski.com/browsers.html> (Nov. 23, 2000).
- [73] See Proxys - 4 - All, *Environmental Variables* at <http://proxys4all.cgi.net/env.shtml> (last viewed Nov. 25, 2000).
- [74] See Privacy Foundation, *Document Based Web Bugs Privacy Advisory* at <http://www.privacyfoundation.org/advisories/advWordBug.html> (Aug. 30, 2000).
- [75] See Steve Silberman, *Is Web-Based Email Bad for Your Anonymity?* at <http://www.wired.com/news/culture/0,1284,10555,10.html> (Feb. 26, 1998).
- [76] See Privacy Foundation, *Document Based Web Bugs Privacy Advisory*, *supra* note 74.
- [77] See Kevin Poulsen, *Scanning the World* at <http://www.securityfocus.com/news/56> (July 7, 2000) (describing the "troubled" and "angry" reaction of system administrators all over the world to the actions of Quova, a California start-up that pinged every assigned, non-governmental IP address this year).
- [78] See Fyodor, *Remote OS Detection via TCP/IP Fingerprinting* at <http://www.insecure.org/nmap/nmap-fingerprinting-article.html> (modified Apr. 10, 1999).
- [79] See Fyodor, *Nmap* at <http://www.insecure.org/nmap/index.html> (modified Oct. 30, 2000).
- [80] See *id.*
- [81] Rik Farrow, *System Fingerprinting With Nmap* at <http://www.networkmagazine.com/article/NMG20001102S0005/1> (Nov. 6, 2000).
- [82] See Fyodor, *supra* note 78.
- [83] See *id.*
- [84] See Sinrod & Williams, *supra* note 58, at 223-24.
- [85] See Back Orifice 2000, *BO2k Comparison* at <http://www.bo2k.com/comparison.html> (July 6, 1999); see also Back Orifice 2000, *A Note on Product Legitimacy and Security* at <http://www.bo2k.com/legitimacy.html> (July 10, 2000).
- [86] See Kevin Poulsen, *NetBus gains Legitimacy* at <http://www.securityfocus.com/news/81> (Sept. 7, 2000)
- [87] See Back Orifice 2000, *A Note on Product Legitimacy and Security*, *supra* note 85 (describing Carbon Copy 32); Anti-AV, *Trojan Chart* at <http://www.antiav.com/chart.html> (Sept. 9, 2000) (cross-referencing commercial and non-commercial remote administration tools, their price, and their information collection capabilities).
- [88] See *In Re RealNetworks Privacy Litigation*, No. 00 C 1366, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May 11, 2000).
- [89] See *In Re RealNetworks Privacy Litigation*, 2000 U.S. Dist. LEXIS 6584.

[90] See Privacy Forum Archive, *Volume 09, Issue 15* at <http://www.vortex.com/privacy/priv.09.15> (May 18, 2000).

[91] See *Supnick v. Amazon.com*, No. C00-0221P, 2000 U.S. Dist. LEXIS 7073 (W.D. Wa. May 19, 2000).

[92] See Keith Perine, *FTC Investigates Amazon's Alexa* at <http://www.thestandard.com/article/display/0,1151,9599,00.html> (Feb. 8, 2000).

[93] See Privacy Foundation, *CueCat Bar Code Reader Privacy Advisory* at <http://www.privacyfoundation.org/advisories/advCueCat1.html> (Sept. 22, 2000).

[94] See Barbara Darrow, *CueCat Pounces On Privacy* at <http://www.techweb.com/wire/story/TWB20000922S0003> (Sept. 22, 2000).

[95] See Simson Garfinkel, *Software that can spy on you* at <http://www.salon.com/tech/col/garf/2000/06/15/broadcast> (Jun. 16, 2000).

[96] See Doug Bedell, *Getting Inside Your Mind* at [http://www.dallasnews.com/technology/174043\\_spyware\\_21per..html](http://www.dallasnews.com/technology/174043_spyware_21per..html) (Sept. 21, 2000).

[97] See *id.*

[98] See Privacy International, *Privacy & Human Rights 2000: Workplace Privacy: Internet and E-mail Usage Boxes* at <http://www.privacy.org/pi/survey/phr2000/threats.html#Heading18> (2000) (describing employer Internet surveillance).

[99] See American Management Association, *Workplace Monitoring and Surveillance* at <http://www.amanet.org/research/monit/monfrm1.htm> (1999).

[100] See WebSense, *The Corporate EIM Vendor Market* at [http://www.websense.com/company/eim\\_market.pdf](http://www.websense.com/company/eim_market.pdf) (Fall 2000).

[101] See U.S. Department of Justice, *Independent Technical Review of the Carnivore System: Draft Report* at [http://www.usdoj.gov/jmd/publications/carnivore\\_draft\\_1.pdf](http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf) (Nov. 17, 2000); see also Cryptome, *Draft Report : Independent Technical Review of the Carnivore System* at <http://cryptome.org/carnivore-rev.htm> (modified Nov. 23, 2000). The Draft Report provides remarkable detail on a secret monitoring system and probably the best look at what government Internet monitoring systems look like.

[102] Regulation of Investigatory Powers Act, 2000, c. 1 (12) (Eng.) available at <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm> (2000).

[103] Cryptome, *U.K. Internet Tapping Bill Stays Intact; Amended Text Addresses Privacy Issues* at <http://cryptome.org/rip-intact.htm> (modified July 17, 2000). To a large extent, RIP appears to resemble ECPA.

[104] See Privacy International, *Privacy & Human Rights 2000: Internet Surveillance and Black Boxes* at <http://www.privacy.org/pi/survey/phr2000/threats.html#Heading9> (2000).

[105] See Cryptome, *Russian Carnivore to Shut Down?* at <http://www.cryptome.org/ru-sormshut.htm> (Sept. 26,

2000).

[106] 480 N.E.2d 552 (Ind. 1985).

[107] *See id.* at 554. "A trespass to a chattel may be committed by intentionally: a) dispossessing another of the chattel, or b) using or intermeddling with a chattel of in the possession of another." RESTATEMENT (SECOND) OF TORTS § 217(1965).

[108] *See id.*

[109] 46 Cal.App.4th 1559 (1996).

[110] *See id.*, at 1563.

[111] *See id.*

[112] *See id.*, at 1564.

[113] *See id.*, at 1566.

[114] *Id.* at 1567 n. 6 (citing *Ream v. Keen*, 838 P.2d 1073 (Or. 1992) (finding trespass to chattels from smoke); *Bradley v. American Smelting and Refining Co.*, 709 P.2d 782 (Wa. 1985) (finding trespass to chattels from microscopic particles); *Wilson v. Interlake Steel Co.*, 32 Cal.3d 229 (1982) (finding trespass to chattels from dust and sound waves); *Roberts v. Permanente Corp.*, 10 Cal.Rptr. 519 (1961) (finding trespass to chattels from dust and sound )).

[115] *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27 (2000).

[116] Nuisance is defined as "that activity which arises from unreasonable, unwarranted or unlawful use by a person of his own property . . . [or] that which annoys and disturbs one in possession of his property, rendering its ordinary use or occupation physically uncomfortable to him." BLACK'S LAW DICTIONARY, *supra* note 2, at 1065.

[117] Burk, *supra* note 115, at 33-34.

The interest of a possessor of a chattel in its inviolability, unlike the similiar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. . . .

Therefore, one who intentionally intermeddles with another's' chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality or value of the chattel . . . Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

RESTATEMENT (SECOND) OF TORTS § 218, cmt. e (1965).

[118] *See id.*, at 34; *see also* RESTATEMENT (SECOND) OF TORTS § 218 (1965).

[119] *See, e.g.,* *America Online v. LCGM, Inc.*, 46 F.Supp.2d 444 (E.D. Va. 1998); *America Online v. IMS, Inc.*, 24 F. Supp.2d 548 (E.D. Va. 1998); *Hotmail Corp. v. Van\$ Money Pie*, No. C98-20064 JW, 1998 U.S. Dist. LEXIS 10729 (N.D. Ca. Apr. 16, 1998); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015 (S.D. Ohio 1997).

[120] *America Online v. LCGM, Inc.*, 46 F.Supp.2d 444, at 451-52; *America Online v. IMS, Inc.*, 24 F.Supp.2d at

550, *Hotmail Corp. v. Van\$ Money Pie*, 1998 U.S. Dist. LEXIS 10729, at \*16, *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. at 1023.

[121] See *CompuServe*, at 1023-24.

[122] *Id.*

[123] *Id.*, at 1024.

[124] 100 F.Supp. 2d 1058 (N.D. Ca. 2000).

[125] See *id.*, at 1069-72.

[126] See *id.*, at 1071. But see *Ticketmaster, Corp. v. Tickets.com, Inc.*, No. CV99-7954-HLH, 2000 U.S. Dist. LEXIS 12987 (C.D. Ca. Aug. 10, 2000) (declining to impose a preliminary injunction, holding instead that a trespass to chattels claim against Tickets.com for the unauthorized indexing of Ticketmaster's web site was preempted by federal copyright law).

It must be said that the trespass question presented and decided in *eBay* bore no resemblance to the trespass question considered by this court on the motion to dismiss last March [because different legal theories were presented]. . . . [I]f taking the information from a publically [sic] available computer was state law trespass, it fell afoul of the preemption aspects of the Copyright Act. . . . It is noted that the harm to [eBay's] equipment foreseen was to its intended function, not the physical characteristics of the computer. A basic element of trespass to chattels must be physical harm to the chattel (not shown here) or some obstruction of its basic function (in the court's opinion not sufficiently shown here).

*Id.* at \*14-15, 16-17.

[127]

[I]t is undisputed that *eBay*'s server and its capacity are personal property, and that *BE*'s searches use a portion of this property. Even if, as *BE* argues, its computer searches use only a small amount of *eBay*'s computer system capacity, *BE* has nonetheless deprived *eBay* of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's property.

*eBay, Inc. v. Bidder's Edge, Inc.*, at 1071.

[128] "A trespasser is liable when the trespass diminishes the condition, quality, or value of personal property. The quality or value of personal property may be diminished even though it is not physically damaged by defendant's conduct." *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 238, 250 (S.D.N.Y. 2000) (quoting *eBay, Inc.*, at 1071).

[129] *Burk*, *supra* note 115, at 34.

[130] See 47 U.S.C. § 227 (2000) (prohibiting all unsolicited advertisements to a fax, cell phone, pager, or other telecommunication device where receiver pays for the call and prohibiting certain unsolicited telephone solicitations, including automated telephone dialing systems).

[131] See *Burk*, *supra* note 115, at 36.

[132] No. 98 AS05067, 1999 WL 450944 (Cal. App. Dep't Super. Ct. Apr. 28, 1999).

[133]

[T]he essential elements of *CompuServe* trespass are readily found in almost any online activity; the cause of action might better be named "using a networked computer." The Internet operates by allowing users to exchange electrons, consume processing cycles, and occupy disc space on its constituent machines. . . . [A]ll that any user needs to fulfill the elements of trespass is to withdraw consent for some real or imagined offense.

Burk, *supra* note 115, at 48.

[134]

*Id.* at 51-52, 53.

[135]

In particular, *Ticketmaster, Corp. v. Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 12987, cited in footnote 126 above, supports Burk's position.

[136]

See Susan M. Ballantine, *Computer Network Trespasses: Solving New Problems with Old Solutions*, 57 WASH. & LEE L. REV. 209, 249-51 (2000).

[137]

*CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015, 1023.

[138]

[After licensing negotiations fell through, Bidder's Edge began to index eBay.] As a result, eBay attempted to block BE from accessing the eBay site; by the end of November, 1999, eBay had blocked a total of 169 IP addresses it believed BE was using to query eBay's system. BE elected to continue crawling eBay's site by using proxy servers to evade eBay's IP blocks.

*eBay, Inc. v. Bidder's Edge, Inc.*, 100 F.Supp. 2d at 1062-63.

[139]

*Hotmail Corp. v. Van\$ Money Pie*, 1998 U.S. Dist. LEXIS 10729.

[140]

*CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015, 1023 (S.D. Ohio 1997).

[141]

133 U.S. 320 (1890); *see supra* note 55.

[142]

*See supra* note 55 & accompanying text.

[143]

*See* GA. CODE ANN. §§ 16-9-93 (a), (b) (1999); MONT. CODE ANN. § 45-6-311 (a) (1999); VA. CODE ANN. §§ 18.2-152.3, 18.2-152.4 (Michie 1996 & Supp. 1999).

[144]

*See* MINN. STAT. § 609.891 (1998).

[145]

*See* WIS. STAT. § 943.70 (West 1996).

[146]

*See* ALASKA STAT. § 11.46.740 (Michie 2000); LA. REV. STAT. ANN. § 14:73.5 (West 1997); MICH. COMP. LAWS §§ 752.794, 752.795 (West 1991 & Supp. 2000); MISS. CODE ANN. § 97-45-2 (2000); S.C. CODE ANN. § 16-16-20 (Law. Co-op. 1985 & Supp. 1998); W. VA. CODE § 61-3C-5 (2000). *Mens rea* means "a guilty mind [or] . . . criminal intent." BLACK'S LAW DICTIONARY, *supra* note 1, at 985.

[147]

*See* ALA. CODE § 13A-8-102 (a) (1994); ARIZ. REV. STAT. § 13-2316 (A) (8) (West 1989 & Supp. 2000); ARK. CODE ANN. § 5-41-104 (a) (Michie 1997); CAL. PENAL CODE § 502 (c) (7) (Deering 1998 & Supp. 2001);

COLO. REV. STAT. § 18-5.5-102 (West 1999 & Supp. 2000); CONN. GEN. STAT. § 53a-251 (b) (1994 & Supp. 2000); DEL. CODE ANN. tit. 11, § 932 (1995 & Supp. 2000); FLA. STAT. ch. 815.06 (1996); HAW. REV. STAT. § 708-892 (1) (Michie 1999); IDAHO CODE § 18-2202 (1997); 720 ILL. COMP. STAT. § 5/16D-3 (West 1998); IND. CODE § 35-43-2-3 (1998); IOWA CODE § 716A.2 (1999); KAN. STAT. ANN. § 21-3755 (1995 & Supp. 1997); KY. REV. STAT. ANN. § 434.850 (Michie 1999); ME. REV. STAT. ANN. tit. 17-A, § 432 (West Supp. 2000); MD. ANN. CODE art. 27, § 146 (1996 & Supp. 1999); MO. REV. STAT. § 569.099 (West 1999); NEB. REV. STAT. § 28-1347 (Michie 1995); NEV. REV. STAT. § 205.4765 (3) (k) (2000); N.H. REV. STAT. § 638:17 (1996); N.J. STAT. ANN. § 2C:20-32 (West 1995); N.M. STAT. ANN. § 30-45-5 (Michie 1997); N.C. GEN. STAT. § 14-454 (b) (1999); N.D. CENT. CODE § 12.1-06.1-08 (1997); OHIO REV. CODE ANN. § 2913.04 (B) (Banks-Baldwin 1997 & Supp. 1999); OKLA. STAT. ANN. tit. 21, § 1953 (1) (West Supp. 2000); OR. REV. STAT. § 164.377 (Supp. 1998); 18 PA. CONS. STAT. § 3933 (Supp. 2000); R.I. GEN. LAWS § 11-52-3 (2000); S.D. CODIFIED LAWS § 43-43B-1 (Michie 1997); TENN. CODE ANN. § 39-14-602 (b) (1) (1997); TEX. PENAL CODE ANN. § 33.02 (West 1994 & Supp. 1999); UTAH CODE ANN. § 76-6-703 (1) (1999); VT. STAT. ANN. tit. 13, § 4102 (1998 & Supp. 2000); WASH. REV. CODE § 9A.52.120 (1998); WYO. STAT. ANN. § 6-3-504 (a) (Michie 1999).

[148] ALA. CODE § 13A-8-101 (11) (1994); ARK. CODE ANN. § 5-41-102 (a) (1) (Michie 1997); CONN. GEN. STAT. § 53a-250 (1) (1994 & Supp. 1999); DEL. CODE ANN. Tit. 11, § 931 (1) (1995 & Supp. 1998); IOWA CODE ANN. § 716A.1 (1) (1999); KAN. STAT. ANN. § 21-3755 (a) (1) (1995 & Supp. 1997); N.H. REV. STAT. ANN. § 638:16 (I) (1996).

[149] ARIZ. REV. STAT. § 13-2310 (E) (1) (West 1989 & Supp. 2000); FLA. STAT. ANN. § 815.03 (10) (1996); KY. REV. STAT. ANN. § 434.840 (Michie 1999); IND. CODE ANN. § 35-43-2-3 (1998); N.D. CENT. CODE § 12.1-06.1-01 (3) (a) (1997); OH. REV. CODE ANN. § 2913.01 (T) (Banks-Baldwin 1997 & Supp. 1999) (the definition for "gain access"); OR. REV. STAT. § 164.377(1) (a) (Supp. 1998); TEX. PENAL CODE ANN. § 33.01 (1) (West 1994 & Supp. 1999); WYO. STAT. ANN. 6-3-501 (Michie 1999).

[150] IDAHO CODE § 18-2201 (1) (1997); MO. ANN. STAT. § 569.093 (1) (West 1999); NEB. REV. STAT. § 28-1343 (1) (Michie 1995) ("to instruct, communicate with, store data in, retrieve data from or otherwise make use of the resources of a computer, computer system, or computer network"); N.J. STAT. ANN. § 2C:20-23 (a) (West 1995); VT. CODE ANN. tit. 13, § 4101 (1) (1998 & Supp. 2000).

[151] See ALASKA STAT. § 11.46.990 (a) (Michie 2000) ("to instruct, communicate with, store data in, retrieve data from, or otherwise obtain the ability to use the resources of a computer, computer system, computer network, or any part of a computer system or network"); 720 ILL. COMP. LAWS 5/16D-2 (West 1998) ("to use, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise utilize any services of a computer"); LA. REV. STAT. ANN. § 14:73.1 (West 1997) ("to program, to execute programs on, to communicate with, store data in, retrieve data from, or otherwise make use of any resources, including data or programs, of a computer, computer system, or computer network"); MD. ANN. CODE art. 27, § 146 (a) (9) (1996 & Supp. 1999) ("to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, computers and other data processing equipment or resources connected therewith"); MICH. COMP. LAWS ANN. §

752.792 (1) (West 1991 & Supp. 2000) ("to instruct, communicate with, store data in, retrieve or intercept data from, or otherwise use the resources of a computer program, computer, computer system, or computer network"); MISS. CODE ANN. § 97-45-1 (2000) ("to program, to execute programs on, to communicate with, store data in, retrieve data from or otherwise make use of any resources, including data or programs, or a computer, computer system or computer network"); NEV. REV. STAT. § 205.4732 (2000) ("to intercept, instruct, communicate with, store data in, retrieve from or otherwise make use of any resources of a computer, network or data."); N.M. STAT. ANN. § 30-45-2 (Michie 1997) ("to program, execute programs on, intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any computer resources, including data or programs of a computer, computer system, computer network or database"); N.C. GEN. STAT. § 14-453 (1999) ("to instruct, communicate with, cause input, cause output, cause data processing, or otherwise make use of any resources of a computer, computer system, or computer network"); R.I. GEN. LAWS § 11-52-1 (1) (2000) ("to approach, instruct, communicate with, store data in, enter data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network"); S.C. CODE ANN. § 16-16-10 (Law. Co-op. 1985 & Supp. 1998) ("to instruct, communicate with, attempt to communicate with, store data in, retrieve data from, or otherwise make use of or attempt to make use of any resources of a computer, computer system, or computer network."); UTAH CODE ANN. § 76-7-702 (1) (1999) ("to directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them"); W. VA. CODE § 61-3C-3 (2000) ("to instruct, communicate with, store data in, retrieve data from, intercept data from, or otherwise make use of any computer, computer network, computer program, computer software, computer data or other computer resources").

[152] See CAL. PENAL CODE § 502 (b) (1) (Deering 1998 & Supp. 2001) ("to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network"); HAW. REV. STAT. § 708-890 (1) (Michie 1999) ("to gain entry to or communicate with a computer, computer system, or computer network"); ME. STAT. REV. ANN. tit. 17-A, § 431 (West Supp. 2000) ("to gain logical entry into, instruct, communicate with, store data in or retrieve data from any computer resource"); OKLA. STAT. tit. 21, § 1952 (1) (West Supp. 2000) ("to approach, gain entry to, instruct, communicate with, store data in, retrieve data from or otherwise use the logical, arithmetical, memory or other resources of a computer, computer system or computer network").

[153] See 18 U.S.C. § 1030 (e) (2) (B) (2000).

[154] See 18 U.S.C. 1030 (a) (2) (C) (2000).

[155] See 18 U.S.C. 1030 (e) (2000).

[156] "Approximately half of the states modeled their statutes primarily on the 1977 or 1979 versions of the proposed 'Federal Computer Systems Protection Act,' while the remainder enacted comprehensive computer assisted crime statutes less closely related to the proposed federal legislation." Laura Nicholson et. al, *Computer Crime*, 37 AM. CRIM. L. REV. 207, 249 (2000).

[157] *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2001).

[158] *Id.*, at 251.

[159] *See id.*

[I]t is clear since at least the date this lawsuit was filed that Register.com does not consent to Verio's use of a search robot, and Verio is on notice that its search robot is unwelcome. Accordingly, Verio's future use of a search robot to access the database exceeds the scope of Register.com's consent, and Verio is liable for any harm to the chattel (Register.com's computer systems) caused by that unauthorized access.

*Id.*, at 249 (citing *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015, 1024 (S.D. Ohio 1997)).

[160] *State v. Rowell*, 908 P.2d 1379 (N.M. 1995).

[161] *Id.*, at 1384.

[162] *Id.*

[163] *State v. Allen*, 917 P.2d 848, 852 (Kan. 1996).

[164] *See id.*, at 853.

[165] *Id.*

[166] *See Moulton v. VC3*, No. 1:00-CV-434-TWT (D.Ga. Nov. 6, 2000), available at <http://pub.bna.com/eclr/00434.htm>.

[167] *See id.*

[168] *Cf. eBay, Inc. v. Bidder's Edge, Inc.*, 100 F.Supp.2d 1058 (N.D. Ca. 2000).

[169] *See* CONN. GEN. STAT. § 53a-251 (b)(2) (1994); N.H. REV. STAT. ANN. § 638:17 (I) (1996); OHIO REV. CODE ANN. § 2913.04 (c) (Banks-Baldwin 1997 & Supp. 1999); W. VA. CODE § 61-3C-17 (a) (1) (2000).

[170] *See* MASS. GEN. LAWS ch. 266, § 120F (West 2000).

[171] *See id.*

[172] N.Y. PENAL LAW § 156.05 (McKinney 1999).

[173] 687 N.Y.S.2d 884, 886 (N.Y. Crim. Ct. 1999).

[174] *Id.* (citing Mem of Attorney-General in support of L 1986, ch 514, 1986 NY Legis Ann, at 233; Governor's Mem approving L 1986, ch 514, 1986 McKinney's Session Laws of NY, at 3173 ["The bill is prophylactic as well as punitive. The computer industry is encouraged ... to devise codes to limit unauthorized use"]; Donnino, Practice Commentary, McKinney's Cons Laws of NY, Book 39, Penal Law art 156, at 284 [device or coding system requirement was incorporated into the law "in order to encourage greater self-protection on the part of the computer industry"]).

[175] *See* STUART MCCLURE ET AL., HACKING EXPOSED: NETWORK SECURITY SECRETS AND SOLUTIONS

51 (1999).

[176] See Section III.B, *supra*.

[177] See Fydor, *supra* note 78; Farrow, *supra* note 81.

[178] See Fydor, *supra* note 78.

[179] See Farrow, *supra* note 81.

[180] See BRUCE SCHNEIER, SECRETS & LIES, DIGITAL SECURITY IN A NETWORKED WORLD 309-312 (2000); LESSIG, *supra* note 6, at 128-30. 138-39.

[181] See Mark Stefik, *Trusted Systems* at <http://www.sciam.com/0397/issue/0397/stefik1.html> (March 1997).

[182]

Authors are wary of entering this market because doing so exposes their works to a higher risk of piracy and other unauthorized uses than any of the traditional, current modes of dissemination. Therefore, authors may withhold their works from this environment. Further, even if authors choose not to expose their works to this more risky environment, the risk is not eliminated. Just one unauthorized uploading of a work onto a bulletin board, for instance -- unlike, perhaps, most single reproductions and distributions in the analog or print environment -- could have devastating effects on the market for the work.

INFORMATION INFRASTRUCTURE TASK FORCE, U.S. DEPT' COM., INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORK GROUP ON INTELLECTUAL PROPERTY RIGHTS 21 (1995) available at <<http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf>>.

[183] See Mark Stefik, *supra* note 181.

[184] See, e.g., Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996); 17 U.S.C. § 1202 (2000).

[185] See Matt Prichard, *How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It*, at [http://www.gameasutra.com/features/20000724/pritchard\\_01.htm](http://www.gameasutra.com/features/20000724/pritchard_01.htm). (Jul. 24, 2000).

[186] See *id.*

[187] The SDMI standard was a watermarking technique that would have interacted with MP3 players and recorders, preventing copying. Researchers at Princeton, the Xerox PARC, and Rice claimed to have found a way to circumvent SDMI. See Edward Felton, *Statement Regarding the SDMI Challenge* at <http://www.cs.princeton.edu/sip/sdmi/announcement.html> (last modified Dec. 1, 2000).

[188] SCHNEIER, *supra* note 180, at 310.

[189] 17 U.S.C. §§ 1201-05 (2000).

However, it is clear that technology can be used to defeat any protection that technology may provide. . . . [T]echnological protection likely will not be effective unless the law also provides some protection for the technological processes and systems used to prevent or restrict unauthorized uses of copyrighted works.

INFORMATION INFRASTRUCTURE TASK FORCE, *supra* note 182, at 2.

[190] See 17 U.S.C. § 1201 (a) (2000).

[191] See 17 U.S.C. § 1201 (b) (2000).

[192] See 17 U.S.C. § 1201 (b) (2000).

[193] See 17 U.S.C. § 1201 (e) (2000).

[194] See 17 U.S.C. § 1201 (f) (2000).

[195] See 17 U.S.C. § 1201 (g) (2000).

[196] See 17 U.S.C. § 1201 (j) (2000).

[197] See 17 U.S.C. § 1201 (i) (2000).

[198] See 17 U.S.C. § 1203 (2000).

[199] See 17 U.S.C. § 1204 (2000).

[200] See 17 U.S.C. § 107 (2000).

[201] See Cohen, *supra* note 184 (Cohen describes how copyright users traditionally have been able to anonymously use lawfully purchased works).

[202]

First Amendment protections [are] . . . embodied in the [Copyright] Act's distinction-between copyrightable expressions and uncopyrightable facts and ideas, and the latitude for scholarship and comment traditionally afforded by fair use . . . [C]opyright's idea/expression dichotomy strikes a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author's expression.

*Harper & Row, Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 546, 556 (1985).

[203] See Cohen, *supra* note 184, at 987-993.

[204] See 65 Fed. Reg. 64555, 64562.

[205] *Id.*, at 64564 (citing *Microsystems Software, Inc. v. Scandinavia Online AB*, No. 00-1503 (1st Cir. Sept. 27, 2000)).

[206] See *id.*

[207] 111 F.Supp.2d 294, 304 (S.D.N.Y. 2000).

[208] See *In Re RealNetworks Privacy Litigation*, No. 00 C 1366, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May 11, 2000); *Supnick v. Amazon.com*, No. C00-0221P, 2000 U.S. Dist. LEXIS 7073 (W.D. Wa. May 19, 2000).

[209] See *In Re American Online, Inc. Version 5.0 Software Litigation*, No. 1341, 2000 U.S. Dist. LEXIS 13262 (J.M. P.L. Jun. 2, 2000).

[210] See Junkbusters, *The Internet Junkbuster Proxy or Guidescope's? Which ad blocking software is right for you?* at <http://www.junkbusters.com/guidescope.html> (Sept. 9, 2000).

[211] See Dwight Silverman, "Adding and Subtracting; With banner ads ubiquitous on the Internet, more software is being developed to block the intrusions," HOUSTON CHRON., Jul. 23, 1999, at 1; Kristi Coale, *Intellicast Smartens Up to Banner Bypass* at <http://www.wired.com/news/technology/0,1282,2844,00.html> (Mar. 28, 1997).

[212] See Janet Cornblum, CNET.com, *Ad filtering catching on?* at <http://news.cnet.com/news/0-1005-200-326551.html> (Feb. 13, 1998).

Website coding and design by [Orlando J. Sanchez](#).

The Journal of Technology Law & Policy or its individual articles may not be distributed by means of the World Wide Web, listserves, distribution lists, newsgroups, or any electronic bulk distribution means without the express permission of the Editor-in-Chief of the Journal. The Journal and its individual articles may be copied by means other than electronic bulk distribution for non-commercial uses provided that the authors and the Journal are credited and identified as copyright holders.

Copyright by the Journal of Technology Law & Policy, a publication by the University of Florida Levin College of Law. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database retrieval system, without prior written permission for the Journal of Technology Law & Policy.