TRADING CYBERSPACES (SEASON II):
An Update of Cyberlaw Relating to Surveillance, Privacy, Security and Domain Names Disputes

27th Annual National Conference on Law and Higher Education
Stetson University College of Law

Nancy Tribbensee
Associate Vice President for Legal Affairs
Arizona State University

Many individuals who work in higher education have noticed that their jobs have taken on the intensity and extreme nature of reality TV shows. In keeping with this theme, the cyberlaw topics to be covered in this paper could be episodes in the following reality TV shows: *Cops, Big Brother, Fear Factor, and The Amazing Race*.

The first section will provide a brief update of CALEA, a federal law that may require colleges, universities, libraries and other institutions to standardize their computing equipment and procedures (at their cost) to facilitate law enforcement use for lawful surveillance. The next section will provide an update of privacy and security issues, legislative attempts to provide protection for consumers, and the implications for colleges and universities. The final section will review processes for responding to unaffiliated websites whose addresses include the unauthorized use of college and university names, mascot references or other trademark indicia.

***COPS*: CALEA and Law Enforcement Access to Computing Systems**

In 1994, Congress passed the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). [1] The Act requires telecommunications carriers to standardize their equipment and procedures to assist law enforcement in executing lawful electronic surveillance.

Initially higher education institutions were exempt from complying with the access capability requirements because they were deemed to be "private networks" which are expressly excluded from CALEA compliance.[2] In the past year, however, the higher education community has had to reconsider the implications of CALEA as the Act has been extended to cover them.

CALEA applies to "telecommunications carriers." A telecommunications carrier is defined as a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire.[3] CALEA requires telecommunications carriers to ensure that their equipment, facilities and services meet "assistance capability requirements" for government access to certain information (pursuant to court order or lawful authorization).[4] These requirements include: isolating individual communications and enabling the government to intercept them, enabling the government to access call-identifying information, and delivering intercepted communications or call-identifying information to the government. The act also requires telecommunications carriers to protect the privacy and security of communications and information that is not

[1] Pub. L. No. 103-414, 108 Stat. 4279
[2] Section 103
[3] Section 102
[4] Section 103

authorized for interception, and to protect information regarding the government's access and interception.

In August 2005, the Federal Communications Commission (FCC)[5] extended CALEA to include facilities-based Internet Service Providers. This extension was made in response to requests from law enforcement. Most campuses are now covered by this extension in their capacity of providing access to the public Internet. The private network exclusion now only applies to networks that do not have the capacity to interconnect with the Internet.

Although the specific technical requirements have not yet been published, representatives of the Higher Education community have objected to this extension of CALEA and the resulting potential impact on college and university computing resources. In April 2004, sixteen educational and library associations filed comments with the FCC objecting to the then proposed extension of CALEA. In October 2005, after the FCC made the extension, the American Council on Education ("ACE")[6] worked with EDUCAUSE and others to file its Petition for Review of the extension. They argued that the FCC and Department of Justice should leave any changes in the law to Congress. ACE argued that law enforcement already has adequate access to campus systems under current law (without any change to CALEA) and that the costs to colleges and universities of compliance would outweigh any benefits to law enforcement. ACE also opined that mandatory compliance with the Act will thwart potential innovations, i.e., that any network improvements would be constrained by CALEA.

---

[5] http://www.fcc.gov/calea/

[6] American Council on Education: acenet.edu

Several colleges and universities have filed requests for exceptions with the FCC. The Higher Education Coalition and other groups are in continuing discussions with the Department of Justice seeking a solution that does not place an undue burden on universities, libraries and schools. Current information about the status of these efforts can be found on the EDUCAUSE and ACE websites.

Big Brother Meets Fear Factor: **Privacy and Security of Information and Computing Resources**

Information resources on campus are our most valuable assets and need to be protected from unauthorized access, alteration and destruction. At the same time, authorized users need to be able to access the information for research, business and legitimate educational uses. Protecting campus information resources will require knowledge of requirements of various state and federal laws. It will also require consideration of fundamental institutional practices, including a review of ways in which information is collected, stored, and accessed.

Much has been written on privacy and security, and EDUCAUSE is an excellent resource for current information in this area.[7] This update will focus on recent developments in state efforts to protect consumer data and thwart or respond to identity theft. It will also describe some employment risk management practices to protect the integrity of campus information resources.

[7] EDUCAUSE (www.educause.edu); see also the Electronic Privacy Information Center www.epic.org) and the Electronic Frontier Foundation (www.eff.org)

The Electronic Privacy Information Center (EPIC) website[8] includes the following summary of recent state laws relating to the privacy of social security numbers:

- A law taking effect in January 2005 in Arizona prohibits the disclosure of the SSN to the general public, the printing of the identifier on government and private-sector identification cards, and establishes technical protection requirements for online transmission of SSNs. The new law also prohibits printing the SSN on materials mailed to residents of Arizona. Exceptions to the new protections are limited. Companies that wish to continue to use the SSN must do so continuously, must disclose the use of the SSN annually to consumers, and must afford consumers a right to opt-out of continued employment of the SSN.

- In California, Senate Bill 168 was signed into law in October 2001. The bill gives individuals the ability to request that a "security alert" be placed on their credit record via a toll-free phone number. The bill also enables Californians to request a "security freeze" that prevents credit agencies from releasing personal information from an individual's credit report. The bill places important restrictions on use of the SSN—public posting of a SSN and printing the SSN on an identity card or document used to obtain a product or service is prohibited. Businesses that use the SSN to identify customers, such as utility companies, will no longer be permitted to print the SSN on invoices or bills sent through the mail.

- California's Senate Bill 1386 went into effect on July 1, 2003. That legislation requires companies that maintain SSNs and other personal information to notify individuals when they experience a security breach. The bill came in response to an April 2002 incident in which the records of over 200,000 state employees were accessed by a computer cracker. The California legislation exceeds federal protections, as there is no national requirement for notice to individuals when personal information is accessed without authorization.

- In June 2004, Colorado Governor Bill Owens signed H.B. 1311 legislation that creates important new protections for the SSN that will take effect later this summer. The new law will limit the collection of the SSN and its incorporation in licenses, permits, passes, or certificates issued by the state. The law requires the establishment of policies for safe destruction of documents

[8] http://www.epic.org/privacy/ssn/

containing the SSN. Insurance companies operating in the state must remove the SSN from consumers' identification cards. Finally, the legislation creates new penalties for individuals who use others' personal information to injure or defraud another person.

- In Georgia, businesses are now required to safely dispose of records that contain personal identifiers. Georgia Senate Bill 475 requires that business records—including data stored on computer hard drives—must be shredded or in the case of electronic records, completely wiped clean where they contain SSNs, driver's license numbers, dates of birth, medical information, account balances, or credit limit information. The Georgia law carries penalties up to $10,000.

Some of these laws may have direct implications for colleges and universities, such as imposing statutory requirements to notify people whose information may have been compromised when university systems are hacked or information is inadvertently disclosed, or to destroy or erase records no longer in use. In addition to legal obligations, when personal data is lost or inadvertently disclosed, institutions also may face more intangible risks. These include public relations issues and the loss of trust by students, employees, consumers, and funding agencies. At a minimum, the statutory requirements can be used as guidelines to develop best practices for policies to respond to inadvertent disclosure of data.

Institutional counsel should be consulted to determine which of the state statutes apply to any given institution (which may require an opinion as to whether the institution is doing business in another state). Regardless of the jurisdictional issues, institutions can begin to develop policies for responding to lost or stolen information based on some of the guidance in these statutes. The policy can serve as a roadmap for offices and departments within the institution

that learn that sensitive information has been lost or disclosed. It should describe who else within the institution should be notified and provide for contacting the police or other law enforcement entities in appropriate cases. It can apply whether the information was stored electronically or on paper or other media.

The policy should provide for timely notice to persons whose records were lost or stolen. That notice can include information relevant to any ongoing investigation, such as the names of college or university contacts, the name of the investigating police officer, and the number of any policy report taken. It can also direct individuals to the FTC website on identity theft[9] and the Social Security Administration fraud line.[10] Numbers for the credit bureaus can also be provided.[11] The purpose of this notification is to allow the affected individual to track credit information and take steps to mitigate any harm.

To reduce the likelihood of an intentional or inadvertent disclosure, higher educational institutions can use basic risk management practices. Everyone has responsibility for protecting the integrity of the campus systems and information. For example, systems should be reviewed to see how often the university is collecting the same sensitive information in multiple departments. In addition, sometimes information is collected when it is not needed or before it is necessary. Each time sensitive information is collected it needs to be protected. In addition, practices regarding employment management and vendor relationships should be reviewed.

---

[9] www.consumer.gov/idtheft
[10] 1-800-269-0271
[11] Equifax 1-800-525-6285, Experian 1-888-397-3742, Trans Union 1-800-680-7289

Institutions can manage some risk through good employment practices. (For the most part, these guidelines apply to student employees and volunteers also.) When new employees are hired (even if they come from other parts of the institution), the supervisor should check their references. Before or as they begin work, the supervisor should provide training on confidentiality, requirements for using computing resources, and security. They should receive orientation on the proper use of protected information (e.g., student and employee records, donor information) and passwords. It may be appropriate to require some employees to sign a statement acknowledging their responsibilities regarding certain data or systems.

As the employee progresses, the department or unit should provide continuing privacy and security training appropriate to the area. As job responsibilities change, through promotion or otherwise, the supervisor should revisit security issues and access privileges. Access to sensitive data, records, systems and equipment should be limited to only those who have a need for access. The supervisor should, in fact, be competent to supervise employees with high-level access to systems. (In other words, the small campus department should not rely on the very competent student worker to access or manage its databases or computing systems unless someone in the department is available to actively supervise.)

In cases in which an employee is about to terminate employment (voluntarily or involuntarily), certain factors should be considered before any negative action is taken or prior to separation. The supervisor should identify the employee’s past

and present access to critical systems or data. It may be appropriate to consult with other administrators, including university counsel, and the chief information officer. Other employees who may be aligned with employee should also be identified. Each institution should develop a protocol for managing the routine termination of employee and student access to data, records, and systems. This might include an automated process for notice to the managers of critical systems for students who are suspended or expelled and employees who are terminated.

Another area for review is vendor and consulting agreements. If they include access to sensitive or confidential information or systems, they should include very specific conditions for access and use. The agreement should describe the relevant description of the sensitive or confidential information and the limits on its use. It should require the return or destruction of all confidential information upon completion or termination of the work under the agreement. Any violation of the confidentiality conditions should constitute a material breach and the confidentiality requirements should survive termination of the agreement. The agreement should also provide adequate insurance and indemnification provisions.

Security decisions, with regard to information technology and otherwise, need to be made in the context of the institution’s primary missions and so should involve representatives from multiple areas of the institution’s administration. Failures can result in university liability and embarrassment if good practices are not in place.

The Amazing Race: **Domain Name Disputes**

College and university administrators are regularly notified of websites that have no authorized affiliation with the institution, but which include a reference to the institution or its mascot in the domain name. The offending website may contain offensive content or may be trying to capitalize on the goodwill developed by the institution. It may be a hate site, a competing site designed to divert content from the institution's legitimate site, or a website developed by a well-intentioned student or alumnus. Often the question becomes: what should be done about the offending site? Domain name disputes are not new, but seem to be increasing at an alarming rate as we all increasingly rely on the Internet for information. This section is included to provide resource information for addressing these issues.

To evaluate the potential for harm and to choose a response when an outsider has used an institutional reference in a website address, the first steps involve viewing the site and considering the use of marks in the address and any additional potentially infringing uses on the site in the context of the institution's policies regarding the use of its trademarks and service marks. In brief, a trademark is a word, distinctive symbol, picture, or slogan used in commerce to identify and distinguish the source of goods or services. The owner of the trademark has the exclusive right to use the mark and the right to prevent the use of a confusingly similar trademark. Trademark rights derive from use of the mark in commerce and are protected under federal and state law. The test for trademark infringement is likelihood of confusion as to origin or sponsorship.

Trademark owners may have a claim for trademark dilution if the mark in question: blurs the distinctiveness of a famous mark, or tarnishes or disparages the famous mark. Failure to prosecute infringers may result in abandonment.

Many colleges and universities have established great value in their institutional marks, earn significant revenues through licensing, and have experience in combating infringers who manufacture or sell t-shirts and other physical items that bear these marks. Website domain names are analogous to trademarks in that they indicate the source of the information contained on the site.

If a review of the site reveals content that may confuse the public as to the source of the information, or it dilutes or disparages an institutional mark, the next step is to identify the person or entity responsible for the site. Sometimes this information is apparent from the website content. Other times it is necessary to research the identity of the party who has registered the domain name for the site.

The Internet Corporation for Assigned Names and Numbers ("ICANN") is a non-profit corporation that coordinates assignment of domain names.[12] ICANN maintains the InterNIC website which lists registration resources, including resources to identify who may have registered an offending site and information about filing complaints.[13] The "Whois" website[14] also provides contact information (name, address) for the registered owner and may reveal other infringing sites.

[12] http://www.icann.org
[13] http://www.internic.net
[14] http://whois.net

EDUCAUSE has responsibility for registering .edu sites for eligible institutions,[15] and can provide registration information for those sites.[16]

All registrars in the .biz, .com, .info, .name, .net, and .org top-level domains follow the Uniform Domain-Name Dispute-Resolution Policy ("UDRP"). To invoke the policy, a trademark owner may (a) file a complaint in court against the domain-name holder (or an action against the domain name if the owner's identity is unknown), or (b) submit a complaint to an approved dispute-resolution service provider.[17]

What if you find a site that is using your name, infringing on your mark or that contains disparaging material? One of the first things you will want to know is the identity of the person or entity that has registered the website. The website http://whois.net provides contact information (name, address) for the registered owner. It may also reveal other infringing sites.

Once the registered owner of the site is identified, the next step is to provide notice to the registered owner, similar to a trademark cease and desist letter. The tone of the letter should take into account the identity of the registered owner (especially if the owner has some affiliation to the institution, such as student or alum or community partner). In some cases the registered owner may offer to sell the offending registration to the complaining institution (and may well have registered it with the intent of profiting from its sale to the legitimate owner of the marks, which is known as "cybersquatting").

[15] http://www.educause.edu/edudomain/
[16] http://whois.educause.net/
[17] http://www.icann.org/udrp

If the letter does not result in informal resolution, you may invoke the remedy provided under UDRP. UDRP provides for an expedited arbitration procedure. [18] The process is inexpensive and entirely electronic. Use of this process does not preclude later litigation.

To prove cybersquatting in a UDRP proceeding, you will need to show that:

1. the Respondent's domain name is identical or confusingly similar to your institution's marks,
2. the Respondent has no right or legitimate interest in using the name,
3. the Respondent has registered the domain name in bad faith, and
4. the registered name is identical or confusingly similar to a distinctive mark (i.e., a mark owned by your institution)

If successful, the UDRP procedure can result in cancellation or assignment of the domain name.

If the institution wants monetary damages in addition to canceling or transferring the domain name, it may file litigation under the federal Anticybersquatting Consumer Protection Act (ACPA). Rather than proving actual damages, the plaintiff may ask the court to award statutory damages of not less than $1000 and not more than $100,000 per domain name.[19] To succeed in an action under the ACPA, the plaintiff will need to show that the defendant acted in bad faith in registering the mark. The court will consider the following factors:

1. the trademark or other intellectual property rights of the defendant, if any, in the domain name;

[18] http://www.icann.org/udrp
[19] 15 U.S.C. § 1117(d)

2. the extent to which the domain name consists of the legal name of the defendant or a name that is otherwise commonly used to identify the defendant;
3. the defendant's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
4. the defendant's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
5. the defendant's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
6. the defendant's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the defendant's prior conduct indicating a pattern of such conduct;
7. the defendant's provision of material and misleading false contact information when applying for the registration of the domain name, the defendant's intentional failure to maintain accurate contact information, or the defendant's prior conduct indicating a pattern of such conduct;
8. the defendant's registration or acquisition of multiple domain names which the defendant knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and
9. the extent to which the mark incorporated in the defendant's domain name registration is or is not distinctive and famous.[20]

The court is not likely to find bad faith if the facts indicate that the defendant has reason to believe that the use of the domain name was a fair use or otherwise lawful.

[20] 15 U.S.C. § 1125(d)(1)(B)

As with non-cyberspace trademark infringers, the institution will not be able or willing to pursue all offending uses of its marks. Registration of obvious institutional references in websites may discourage infringers and more importantly, help members of the public who are searching for the institution to arrive at the correct destination. When appropriate, however, institutional marks will need to be protected through the use of UDRP or ACPA processes.

CONCLUSION

Over the next year, higher education institutions are encouraged to watch for developments regarding the applicability of CALEA, and perhaps participate in support of the national efforts in this arena. In addition, we should expect to see an increasing number of state and federal laws intended to address the identity theft epidemic, but none of the legislation will have its intended effect if institutional practices are not changed. Finally, institutions can measure their success by the number of websites that infringe on their marks and will need to develop internal policies for deciding which will merit response. In other words, as reality TV goes, no one is likely to win a big cash reward or be voted off the island, but these shows are guaranteed to be in the line-up for years to come.