Global Information Assurance Certification Paper

The State of Digital Copyrighting
Keith Filzen
17 February, 2001

There are literally millions of digitally stored documents, pictures, and music media accessible via the Internet. If it can be transferred a digital format it is most probably available on the Internet. I would venture to say, no that's to weak, I guarantee that a good percentage of the data available digitally could be classified as copyrighted or copyrightable material.

Movies you watch at home either purchased or rented have a Federal Copyright notices at the beginning. Pre-recorded videos have analog encoding that is used to deter people form making copies. Is it hard to get around? No. For many years hardware has been available to make analog copies overcoming built in the protection. And, just recently I purchased a digital VCR that overcomes the protection due to the fact that a copy is made using the digital output.

Audio, and software CD's have symbols such as: ® ©™, which all imply some type of registration for ownership rights and imply penalties for unauthorized transfer. Usually accompanying these symbols are statements such as "All Rights Reserved" or "Unauthorized duplication is a violation of applicable laws."

DVD's because of their digital format were afforded a strong encryption scheme to prevent unauthorized duplication. The encryption employed seemed like a magnet to the online community interested in testing such deterrents. It didn't take very long to break and publish the key.

Then there's the Napster/gunitella ordeal, and MP3 audio, as well as intellectual property from commercial companies, and educational materials and papers, not to mention electronic publishing and software.

Protecting intellectual property is a core requirement of the e-business infrastructure. So what is the online community supposed to do to conduct business in an ethically and morally correct manner? Identify, protect, monitor and prosecute. That is after everyone can agree upon common laws and technology though.

What defines the current state

The Internet needs a solution to protect and identify ownership of media. This is a global issue not specific to the United States for which the European community is especially sensitive. In fact, the European community requires much more stringent requirements for the release or dissemination of information and products than in the United States.

This effort is being addressed by a number of initiatives in the United States starting with PDD-63, the Presidential Decision Directive to protect America's critical infrastructure(s) and assure the security of the United States' increasingly vulnerable and interconnected

infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services. Organizations such as the Center for Internet Security, the FBI and it's Infraguard program, NIST, the Department of Commerce's Safe Harbor self certification program to meet European "adequacy" standards for privacy enabling uninterrupted e-business with the European community, and SANS just to name a few. These organizations are committed to collaborative efforts to use best practices and standards to educate and secure Internet activities.

The United States government understands the problem and is instituting regulations and laws to help safeguard the rights of data owners. Consequently so is the European. Can't we all just get along?

H.R.354, sponsored by Rep Coble, Howard, Chairman of the Courts and Intellectual Property Subcommittee, introduced this bill in January of 1999 focused on amending title 17, United States Code, to provide protection for certain collections of information. The Collections of Information Antipiracy Act, amends Federal copyright law to make liable to the injured party anyone who makes available to others a substantial part of a collection of information gathered or maintained by another person through the investment of substantial resources, so as to harm the other person's (or a successor's) primary or related market for a product or service that incorporates such information and is offered or intended to be offered in commerce.

It also provides that protection shall not extend to information gathered or maintained by or for a government entity, to computer programs, or to digital online communications. It stipulates that nothing in this Act shall limit, impair, or annul in any manner the protections under Federal or State law or regulation relating to the collection or use of personally identifying information, including medical information.

The bill is supported by businesses which create content (such as Reed-Elsevier, Thomson, and IBM), but opposed by businesses such as Yahoo!, Bloomberg and E-Trade and academics that republish other people's database content, and don't want to pay for it.

The Digital Millennium Copyright Act (DMCA) represented the most comprehensive reform of United States copyright law in the past generation. DMCA referenced as H.R.2696, S.2037, became Public Law No: 105-304 on October 28, 1998 and was amended to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty ratification of the World Intellectual Property Organization (WIPO) treaties.

Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider (OSP) liability, including details on safe harbors, damages, and "notice and takedown" practices.

The U.S. Copyright Process, under Title 17, allows authors a number of relatively long-duration but limited-extent, exclusive rights to their original works that are within

specific categories of copyrightable subject matter. Current recognized categories of copyrightable subject matter reflect the current awareness of tangible works. The list of current categories is statutorily recognized to be open-ended and to include:

(1) Literary works, which include computer programs;
(2) Musical works, including any accompanying words;
(3) Dramatic works, including any accompanying music;
(4) Pantomimes and choreographic works;
(5) Pictorial, graphic, and sculptural works;
(6) Motion pictures and other audiovisual works;
(7) Sound recordings, and
(8) Architectural works.

The Problem

Most readily available or widely distributed technologies employed for the purpose of copyrighting media are week and easily broken. Use of digital media on the Intenet is not well defined, and most people think if they can access and download media that it is free.

Here are some examples of things that are usually acceptable uses of others Internet sites:

> Downloading a file, image or material that is openly accessible to your home computer for your personal information. The insertion of text-based links to information available form other sites, on you own. The printing of a single copy of any accessible webpage or data contained within for your own personal use. Email or use of the "send page" feature of your browser to send a single copy of a file to a friend/family member.

Here are some examples of things that are usually unacceptable uses of others Web sites:

> The insertion of anything on a web page other than a link to other sites information. Reproduction of materials within any commercial publication or for any commercial purpose. The printing of more than a single copy for your personal use. Reproduction of any image, audio, or videos from other sites.

The web is one of the last places that you can get something for free. It is an excellent medium to distribute media, but there's one problem in that valuable intellectual property, once exposed on the Web, is easily accessible, and most protection mechanisms are easily compromised.

The inability classify digital files and track the flow of files as they traverse geographic boundaries providing the ability to identify their source and possibly a chain of custody could be a valuable technology. Unfortunately, to most it would be an invasion of privacy.

Such benefits could help diagnose accidental or unauthorized transmit of media, and alert to sanitation or alteration. The electronic inventory of digital media has many implications not the least of which is prosecution support.

Who Should Be Concerned?

Everyone who has something available that is deemed to be worth something. That's a pretty broad statement I know, but I think that everyone with Internet access will at one time feel the need to protect something that they value and is accessible via the Internet..

Industry Trends

Proprietary solutions are standard, and if you're not familiar with proprietary solutions, they're usually expensive and cumbersome to use. Not to mention that they are readily sold, bought out, or go out of business and you lose support.

Encryption has long been the most prevalent solution and one that provokes a considerable amount of attention and resources to be the first to break it.

Providing the ability to perform both covert and covert analysis and tracking of media, in hopes of dissuading and/or catching those individuals performing unethical acts is a prevalent theme.

Promising solutions

Organizations are demanding ways to make valuable intellectual property available for sale or controlled distribution via the Internet. For organizations whose product is intellectual property, the need to protect that property from inappropriate use becomes much more important as traditional distribution mechanisms give way to the Web.

The Gartner Group presented some assumptions as to E-commerce solutions to protect intellectual property and are that the publishing and music industries will drive the use of some form of Digital Right Management (DRM) and that enterprises adopting e-commerce strategies that use or provide digital content will use some type of secure content delivery tools or services in the near furtue.

Whatever the technology employed, it should be of universal simplicity. Watermarking is on such technology that works with all types of media, both digital and tangible. The concept leads to the basics of Stenography, and therefore capitalizes on the broad work with associated implementation strategies such as; spread spectrum, noise theory, microdots, covert channels and IP headers, spatial organization, and time or frequency domains.

Of the many technologies available there are some common elements to be addressed that are of universal appeal and include:

1. Should be able to identify the source;
2. Should be able to provide copyright information;
3. Should be able to survive photocopy/faxing;
4. Should be printer independent;
5. Should be able to track distribution, augmenting the original source;
6. Should provide the ability to deploy Non-washable classifications;
7. and, Should be able survive reformatting or compression

Some vendors have created proprietary solutions such as Epson for its digital cameras, via a software add-on called the Image Authentication System (IAS), which installs software in the camera that adds an encrypted key to each image. The key is said to be quite sensitive where changing even a single pixel will cause the image to fail authentication and alert you if the image has been altered.

Among the many references to technology one acronym seems to stand out as a solution that is shared by some key players and that is DRM or Digital Rights Management. DRM is defined as the trusted exchange of digital information over an Intranet, extranet, or the Internet, and controls users' rights once they have a file. Users are granted only the privileges the media sender allows. A key characteristic of DRM is the *persistent* protection of this information. Protection does not stop once the user receives the information but follows the information throughout its use. DRM can control the type of access granted to the user of the information, protecting the information from being copied, printed, or redistributed without permission

DRM technologies control the use of electronically distributed documents, graphics, audio, and video files, and is a subset of secure content technologies. While the need to protect intellectual property is a concern for businesses moving their operations to the Web, the initial markets for DRM are focused on the need to manage information being distributed and purchased by consumers.

Secure content applications protect content transmitted over the Internet. The components of secure content offerings include encryption, guaranteed e-delivery, rights management records management, non-repudiation.

Applications employing DRM are emergent technologies, and are prime for the publishing industry and early adopters wanting to curtail the loss of revenue to the secondary markets for book sales as an example. Some of the vendors promoting DRM solutions are Adobe's PDF Merchant, ASPSecure, Authentica, ContentGuard, IBM, Infraworks, InterTrust, PublishOne, Reciprocal, and Softlock.

Circumventing solutions

A major question that will be resolved over the next couple years is whether consumers are truly willing to pay for high-value content. Corporate consumers who need the high-value content as part of their job will not be bothered because the corporation will pay the bill. Consumers may just ignore it all together.

Where there's a will there's a way. The current state affairs with responsibility and retribution for criminal activity on the Internet is weak to say the least, and crosses so many geography and cultural barriers that it's almost impossible to control.

Early implementations of technologies such as watermarking could be easily washed or cleansed. Images and data that are typically compressed can lose identifiable properties once compressed, and most solutions require text to be treated as a picture to achieve desired results.

Where do we go from here?

Current technological advancements are not enough by themselves to protect digital media. International collaboration on standards and best practices need to be employed and a common criteria developed. As previously stated, technology is not the end all solution. Education has to play an important part of the equation and needs to be addressed to alert everyone as to the risk, and consequences of their action in hopes of creating an ethically aware culture.

The flip side to any education program are the basic building blocks like reading, righting and arithmetic. In the case of digital copyrighting, it is the laws and policies that provide the underlying foundation. The laws and policies need to be far reaching, and thus international in flavor. Of all the efforts to date, the World Intellectual Property Organization (WIPO), an international organization that is one of the 16 specialized agencies of the United Nations that administers 21 international treaties dealing intellectual property protection, is dedicated to promoting the use and protection of works of such property.

The treaties define internationally agreed upon basic standards for intellectual property protection, and registration treaties, ensuring that a single international registration or filing will have effect in any of the 175 member nations.

Conclusion

What is needed is an industry standard by which everyone can identify. The trick is how can it be done on the Internet where the culture does not reflect everyday reality. Laws are hard to enforce on the Internet. The issue of taxation is prime example of basic economic concepts still going on and does not appear to be going anywhere.

We could use monitoring tools and regulate the Internet, which I think everyone disagrees with, well almost everyone, and would stifle the creativity and flow of society. The mere fact that users of the Internet are able to impersonate other individuals demonstrates that there are much bigger issues to resolve and put forth efforts.

It really comes back to a universally recognized way of classifying and marking media but with digital technology. I say universally because the Internet is universal and

therefore helps fuel the problem. Actions performed by an individual nation may or may not be recognized by another, and most definitely not by all without some world organization intervening. Even then, with the state of some nations at war with others, there are no real safeguards.

The other side of the coin is users themselves. They must be educated. I have done some research on the subject of the Internet within secondary schools in the United States and in some instances they have implemented education programs prior to allowing access to computer systems. Within PDD-63 there are references to morality and providing for the integration of acceptable use of computer systems and the Internet. It's a start.

References

1. The Journal of Electronic Publishing. Volume 6, Issue 2. December, 2000.
   URL: http://www.press.umich.edu/jep

2. Harper, Georgia. "**Copyright Endurance & Change.**" *EDUCAUSE Review*.
   Volume 35, Number 6, November, 2000.
   URL: http://www.educause.edu/pub/er/erm00/articles006/erm0062.pdf

3. **Digital Millennium Copyright Act**
   URL: http://www.adobe.com/prodindex/acrobat/readstep.html

4. Machrone, Bill "Digital image authentication hits the consumer Market." EWeek.
   April 26, 1999
   URL: http://www.zdnet.com/eweek/stories/general/0,11011,400396,00.html

5. Gilbert, Weintraub "Protect intellectual property with digital rights management technology." TechRepublic. November 22, 2000

6. Degnan, Chrsta, "To serve and protect documents." EWeek.
   September 12, 1999
   URL: http://www.netvoyage.com/press/pcweek1.htm

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event