STATE BAR OF MICHIGAN

MICHIGAN COMPUTER LAWYER

State Bar of Michigan Computer Law Section http://www.michbar.org/computer/ Volume 22, Issue 3

Contents

Michigan Computer Lawyer is published bi-monthly. If you have an article you would like considered for publication, send a copy to:

Matthew M. Jakubowski
Brooks Kushman, PC
1000 Town Center
Floor 22, Suite 2200
Southfield, MI 48075-1183
E-Mail: mjakubowski@brookskushman.com

CAN SPAM Act

By Dante M. Benedettini

I Don't Want To Enlarge My Genitals, Take Viagra, or Lose 100 Pounds in 10 Days: Spamming the 6th Circuit; Are There Adequate Statutory Laws and Remedies Available In the 6th Circuit Against Spam?

Dante Benedettini was the First Place Winner of the 2004 Edward F. Langs Writing Award with the following paper on the CAN SPAM act. A graduate of the University of Detroit Mercy School of law, Dante is employed in the Detroit office of Berry Moorman, where he has worked for 2 1/2 years, first as a Law Clerk, then as an attorney. He practices in the Business & Corporate, Civil Litigation, Labor & Employment, and Real Estate practice groups, where he conducts transactional and litigation work in the areas of construction, real estate, debt collection, computer and internet issues, and bankruptcy. Dante will speak on the CAN SPAM Act at the Computer Law Section's upcoming Spring Networking Event on May 19, 2005.

Spam or Unsolicited Commercial E-mail (UCE) has become a serious problem over the past several years. As Oliver Wendell Holmes said "The life of the law has not been logic, but experience." In response to UCE, laws have developed in every state to combat UCE. Congress has also acted upon the threat of UCE and passed legislation attempting to deal with it. Many believe these federal laws to be ineffective against Spammers[1] based upon the statutes' language. Does Congress's attempt to preempt the states anti-UCE statutes seriously undermine 6th Circuit residents from adequate protection against spammers?

The first part of this paper will attempt to explain what UCE is, how people get e-mail addresses in order to send UCE to their e-mail box, and

what problems UCE causes. The second part of this paper will then analyze whether the laws, both state and federal, within the 6th Judicial Circuit provide Internet users with adequate protection and remedies against UCE.

UCE; What Exactly Are We Dealing With?

We all go through the annoying and frustrating process of checking our e-mail and finding several, sometimes dozens, of unwanted e-mail solicitations clogging up our boxes. These e-mails are usually advertisements for goods and services that we don't want or need. Sometimes they can be downright offensive including pornographic terms or language in the subject line of the message. This paper will explain what UCE is and how it really works. After this explanation it will inquire whether there is an adequate remedy at law in the 6th Judicial Circuit for Internet users who are plagued by UCE.

What exactly is UCE?
Why Is It Called Spam?

The name Spam is of course synonymous with the canned meat product offered by Hormel. It is unclear how it became linked with unwanted e-mail messages in popular culture but there are two main theories. The first theory is that the name was borrowed from the British television series *Monty Python's Flying Circus*. In a skit on that program the actors sang a song entitled "Spam" which consisted of the word "Spam" sung over and over, annoyingly drowning out all other sounds. People began to associate this with e-mail messages because it was so similar; a large number of messages being sent to a receiver and annoyingly drowning out all other messages. The second theory simply compares e-mail Spam to the actual lunchmeat. No one wants it, it is unpleasant to look at, and it always seems to be available.

How Do You Define UCE?

Some people define UCE broadly as unsolicited e-mail from any source and for any purpose. However, if a long-lost friend or relative finds your e-mail address and sends you a message, this could hardly be called UCE, even though it's unsolicited. UCE is generally e-mail advertising for some product sent to an e-mail mailing list[2] or newsgroup[3]. UCE usually comes from a commercial sender for a commercial purpose, which leads some to call UCE by another name, unsolicited commercial e-mail or UCE.

There are several acronyms used to refer to Spam. The four most popular are as follows:

UBE or Unsolicited Bulk E-mail – E-mails with substantially identical content sent to many recipients who have not asked for them. It should be noted that all UBE is UCE but not all UCE is UBE. It is simply a quantitative term. UCE's sent in bulk are then termed UBE's.

UCE or Unsolicited Commercial E-mail – (as stated above) E-mail containing commercial information that has been sent to a recipient who did not ask to receive it.

MMF or Make Money Fast - Messages that "guarantee immediate, incredible profits!" including such schemes as chain letters.

MLM or Multi-Level Marketing - Messages that "guarantee incredible profits!" right after you send them an "initial investment" and recruit others.[4]

How Do I Get UCE or How Does UCE Make It To My E-mail Box[5]?

"I didn't sign up for this junk," you say. "Why am I being sent so much UCE?" The answer is almost unbelievable. Those who send UCE or "Spammers," use several methods of obtaining e-mail addresses. These methods sound like something out of science fiction stories.

Spammers regularly scan UseNet[6] for e-mail addresses, using ready-made programs designed to do so. Some programs just look at articles' headers which contain e-mail addresses (From: xxx, Reply-To: xxx, etc), while other programs check the articles' bodies, by using programs that look at signature lines or anything else that may contain an '@' character and attempt to demunge munged[7] e-mail addresses from that information.

Spammers regularly attempt to get a list of subscribers to a mailing list (some mail servers will give those upon request), knowing that the e-mail addresses are unmunged and that only a few of the addresses are invalid. When mail servers refuse or are electronically configured to refuse such requests, another trick might be used. Spammers might send an e-mail to the mailing list with the headers *"Return-Receipt-To: <spammer's e-mail address>"* or *"X-Confirm-Reading-To: <spammer's e-mail address>."* Those headers would cause some mail transfer agents and reading programs to send an automatic verification e-mail back to the *<spammer's e-mail address>*, in the header, saying that the e-mail was delivered to *<an e-mail address of one of the subscriber's>,* thereby divulging that address to spammers.

A different technique used by spammers is to simply request a subscriber/mailing list server to give them a list of all the mailing lists it carries (an option implemented by some mailing list servers for convenience of legitimate users), and then send the UCE to one or all of the mailing list's addresses, leaving the server to do the hard work of forwarding a copy to each subscribed e-mail address.

Spammers have programs which crawl through web pages, looking for e-mail addresses, especially those that are contained in "mailto:" HTML[8] tags (those highlighted e-mail addresses on a web page that you click on and a mail window opens allowing you to compose a message to that e-mail). These programs are referred to generally as "address harvesters." They are also referred to as robots (or bots), spiders, and/or crawlers. These programs are quite alarming because they have the capability of searching over thousands of web pages and harvesting large numbers of e-mail addresses. This is especially troublesome for individuals or businesses, which offer advertising for their goods or services on the Internet through a web page because they need to provide e-mail addresses for their customers on these sites. The Spammers harvest these addresses and add them to their UCE lists, eventually clogging up the e-mail boxes of these web page owners.

These tactics especially plague Law firms, accounting firms, medical offices, and other professional service businesses. Since these professionals are usually required to place their e-mails on their web sites for contact purposes, their e-mail address is easy prey to the Spammers' harvesters. These professionals' day-to-day operations are now taxed because of the time it takes to comb through their e-mails in order to separate the UCE from the legitimate e-mail. If you are a law firm with UCE problems you may want to munge the addresses on your website. This may cut down on some UCE.

There are various sites that serve as "white pages"[9], sometimes named people finders web sites. For example the famous Yellow Pages now has an e-mail directory on the Internet offering people searches by e-mail address. These white/yellow pages contain addresses from various sources, for example from UseNet.

Sometimes, however, an e-mail address will be registered automatically with a white page directory. For example Microsoft Network's HotMail will add e-mail addresses to Bigfoot Communications[10] by default, making new addresses available to the public. Spammers go through those directories in order to get e-mail addresses. Most directories prohibit e-mail address harvesting by spammers, but because those databases have large numbers of e-mail addresses and names, it's a tempting target for spammers.

There are two types of lists. The first type, "harvested," consists of buying a list of e-mail addresses (often on CD) that were harvested by other methods, for example someone harvesting e-mail addresses from

UseNet then sells the list either to a company that wishes to advertise via e-mail (sometimes passing off the list as that of people who opted-in for e-mailed advertisements) or to others who resell the list. The second type, "compiled," consists of a company who gets the e-mail addresses legitimately (e.g. a magazine that asks subscribers for their e-mail in order to keep in touch over the Internet) and sells the list for the extra income. The compiled list includes e-mail addresses a company gets by any and all other possible means as well. For example someone who e-mails a company with inquiries regarding any context like customer service or technical support. This makes one think the next time they request help online.

> Some web sites use various tricks to extract a web surfer's e-mail address from their web browser[11], most of the time without the surfer even noticing it. Those techniques include:
> 1. Making the web browser fetch one of the page's images through an anonymous FTP[12] connection to the site. As default some browsers will give the e-mail address the user configured[13] into the web browser as the password for the anonymous FTP account. A surfer unaware of this technique will fail to realize that their e-mail address has been compromised.
> 2. If an e-mail address is configured into the user's web browser the spammer can use JavaScript[14] to make that user's browser send an e-mail to the spammer's e-mail address. This would of course give the spammer the user's e-mail address in the "From:" line of the message. Some browsers will automatically trigger an e-mail to be sent when the mouse simply passes over some part of a page. Unless the browser is properly configured, no warning will be issued.
> 3. Using the "HTTP_FROM" header that browsers send to the server. Some web browsers pass a header with your e-mail address to every web server you visit.
> It's worth noting that when one uses a web browser to read their e-mail (or any mail reader that understands HTML), the reader should be aware of any active content (Java applets[15], JavaScript, Visual Basic or VB[16], etc) as well as web bugs[17] as they are tools spammers use to obtain e-mail addresses. Also, an e-mail containing HTML may contain a script[18] that when read automatically will send an e-mail from the reader to a specified e-mail address. A good example of this case is the Melissa virus[19]. Such a script can send the spammer not only the reader's e-mail address but also all the addresses on the reader's address book.

Every domain name has one to three contact points[20]; administration, technical, and billing. These contact points usually include the e-mail address of the contact person. As the contact points are freely available[21] spammers harvest the e-mail addresses from the contact points for lists of domain names. This is a tempting method for spammers, as those e-mail addresses are most usually valid and mail sent there is being read regularly.

There are of course others besides the above-mentioned seven, however these are the most popular methods. Of course, due to the nature of technology and the Internet itself, more methods will most likely develop in the future allowing e-mail addresses to continue to fall prey to Spammers.

So what's The Problem with UCE?

In addition to wasting people's time with unwanted e-mail, UCE also eats up a lot of network bandwidth[22]. Bruce Miller runs the website www.aboutspam.com. Miller is a self-proclaimed anti-spam activist. He has articulately illustrated the potential nuisance and harm from "innocent" UCE. On his website Miller explains:

> According to the World Book Encyclopedia, 2001 Edition, Volume B, page 724, there are 15,000,000 single proprietorship business, 1,500,000 partnerships, and 4,000,000 corporations in the United States. Add them all together and you get 20,500,000 businesses. If each of these businesses sent you one e-mail and you wanted to opt out of future e-mails for each of these businesses, the 22 seconds to opt out suddenly becomes quite a time-consuming affair: 451,000,000 seconds, or 7,516,666 minutes, or 125,278 hours, or 5,220 days, or 14.3 years opting out. You'll be spending all your time opting out instead of reading your personal e-mail.
>
> Now, let's consider the size of each UCE. Here are the sizes in kilobytes of my last 20 UCE's at the time I began writing this page:
>
> 11.90, 3.90, 3.60, 6.80, 11.00, 11.00, 4.80, 1.60, 18.00, 2.20, 4.50, 3.20, 2.00, 5.00, 3.20, 2.90, 12.00, 2.80, 18.00, 3.80. Total: 131.30 kb Mean Average: 6.565 kb.
>
> The typical amount of storage space an ISP provides for the storage of e-mail on its server is 2 or 3 megabytes. Let's use 2 megabytes, or 2,000,000 bytes, which is the amount offered on Hotmail and because Hotmail is a very popular e-mail service. Using the average UCE size of 6,565 bytes, simple math shows this: 2,000,000/6,565 = 304.6 messages. Let's round to 307 messages. It will only take 307 messages to fill up your e-mail account. When it is filled up with UCE, all other e-mail -- wanted or not wanted -- will be rejected.
>
> (Quoted with permission) http://www.aboutspam.com/index.php.

The above quote from Miller illustrates that both time and storage space are compromised by UCE. Time and storage space equal money. UCE saps our system resources and it saps storage space in our mailboxes. The recently passed *Controlling the Assault of Non-Solicited Pornography and Marketing Act* of 2003 or CAN-SPAM Act of 2003 contains similar conclusions. In 15 USCS § 7701(2) of that Act entitled Congressional Findings and Policy, Congress states that:

> The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently [in 2002] estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise.

Many people have tried to summarize the problems that UCE pose for all of us. One of the best sources for these summaries is organizations that know technology and specialize in the knowledge of UCE and Spamming techniques. Several such organizations were formed over the last several years to combat UCE. One of these organizations is the *Coalition Against Unsolicited Commercial E-mail* or CAUCE[23]. This organization's homepage states that the CAUCE was "created by [citizens of the Internet] to advocate for a legislative solution to the problem of UCE (a/k/a "Spam")." While not a legal authority, this organization is quite "tech-savvy" and has summarized what it thinks are the main five problems with UCE. The website states:

Cost-Shifting

Sending bulk e-mail is amazingly cheap. With a 28.8 dialup connection and a PC, a spammer can send hundreds of thousands of messages per hour. Sounds great, huh? Well, it is for the spammer. However, every person receiving the spam must help pay the costs of dealing with it. And the costs for the recipients are much greater than the costs of the sender.

Some junk e-mailers say, "Just hit the Delete key!" Unfortunately, the problem is much bigger than the time and effort of one person deleting a couple of e-mails. There are many different places along the process of transmitting and delivering e-mail where costs are incurred. In the Internet world, "time" equals many different things besides the hourly rate that many people are still charged.

For example, for an Internet Service Provider, "time" includes the load on the processor in their mail servers; "CPU time" is a precious commodity and processor performance is a critical issue for ISPs. When their CPUs are tied up processing spam, it creates a drag on all of the mail in that queue -- wanted and unwanted alike. This is also a problem with "filtering" schemes; filtering e-mail consumes vast amounts of CPU time and is the primary reason most ISPs cannot implement it as a strategy for eliminating junk e-mail.

The problem is also compounded by the fact that ISPs purchase bandwidth -- their connection to the rest of the Internet -- based on their projected usage by their prospective user base. For most small to mid-sized ISPs, bandwidth costs are among one of the greatest portions of their budget and contributes to the reason why many ISPs have a tiny profit margin. Without junk e-mail, greater consumption of bandwidth would normally track with increased numbers of customers. However, when an outside entity (e.g., the junk e-mailer) begins to consume an ISP's bandwidth, the ISP has few choices: 1) let the paying customers cope with slower internet access, 2) eat the costs of increasing bandwidth, or 3) raise rates. In short, the recipients are still forced to bear costs that the advertiser has avoided.

"Time" also makes for some other interesting problems, especially coupled with volume. Recent public comments by AOL are a useful point of reference: of the estimated 30 million e-mail messages each day, about 30% on average was unsolicited commercial e-mail [that's 9 million e-mails per day]. With volumes such as that, it's a tremendous burden shifted to the ISP's to process and store that amount of data. Volumes like that may undoubtedly contribute to many of the access, speed, and reliability problems we've seen with lots of ISPs. Indeed, many large ISPs have suffered major system outages as the result of massive junk e-mail campaigns. If huge outfits like Netcom and AOL can barely cope with the flood, it is no wonder that smaller ISPs are dying under the crush of spam.

Fraud

Spammers know that in survey after survey, the overwhelming majority (often approaching 95%) of recipients don't want to receive their messages. As a result, many junk e-mailers use tricks to get you to open their messages. For instance, they make the mail "subject" look like it is anything other than an advertisement.

In many cases, ISPs and consumers have set up "filters" to help dispose of the crush of UCE. While filters often consume more resources at the ISP, making mail delivery and web surfing slower, they can sometimes help end-users cope a little bit better. Spammers know this, so as they see that mail is being blocked or filtered, the use tricks that help disguise the origin of their messages. One of the most common tricks is to relay their messages off the mail server of an innocent third party. This tactic doubles the damages: both the receiving system and the innocent relay system are flooded with junk e-mail. And

for any mail that gets through, often times the flood of complaints goes back to the innocent site because they were made to look like the origin of the spam. Another common trick that spammers use is to forge the headers of messages, making it appear as though the message originated elsewhere, again providing a convenient target.

Waste of Others' Resources

When a spammer sends an e-mail message to a million people, it is carried by numerous other systems en route to its destination, once again shifting cost away from the originator. The carriers in between are suddenly bearing the burden of carrying advertisements for the spammer. The number of spams sent out each day is truly remarkable, and each one must be handled by other systems; there is no justification for forcing third parties to bear the load of unsolicited advertising.

The methods employed by spammers to avoid being held responsible for their actions are very often fraudulent and tortious. Numerous court cases are underway between spammers and innocent victims who have been subjected to such floods. Unfortunately, while major corporations can afford to fight these cutting edge cyber law battles, small "mom-and-pop" ISPs and their customers are left to suffer the floods.

There's a long tradition in this country of making commercial enterprises bear the costs of what they do to make money. For example, it would be far cheaper for chemical manufacturers to dump their waste into the rivers and lakes... however "externalities" (as the economists call it) are bad because they allow one person to profit at another's -- or everyone's -- expense.

The great economist Ronald Coase won a Nobel Prize talking about exactly this kind of situation[24]. He said that it is particularly dangerous for the free market when an inefficient business (one that can't bear the costs of its own activities) distributes its costs across a greater and greater numbers of victims. What makes this situation so dangerous is that when millions of people only suffer a small amount of damage, it is often more costly for the victims to go out and hire lawyers to recover the few bucks in damages they suffer. That population will likely continue to bear those unnecessary and detrimental costs unless and until their individual damage becomes so great that those costs outweigh the transaction costs of uniting and fighting back. And the spammers are counting on that: they hope that if they steal only a tiny bit from millions of people, very few people will bother to fight back.

In economic terms, this is a prescription for disaster. Because when inefficiencies are allowed to continue, the free market no longer functions at peak efficiency. As you learn in college Microeconomics, the "invisible hands" normally balance the market and keep it efficient, but inefficiencies tip everything out of balance. And in the context of the Internet, these invisible marketplace forces aren't invisible anymore. The inefficiencies can be seen every time you have trouble accessing a web site, or whenever your e-mail takes 3 hours to travel from AOL to Prodigy, or when your ISP's server is crashed by a flood of spam.

CAUCE believes that stealing is stealing, whether you take a penny or a dollar or a thousand dollars. Remember, you only need to steal a penny from 4 million people in order to have enough to buy yourself a brand new Mercedes Benz.

Displacement of Normal E-mail

E-mail is increasingly becoming a critical business tool. In the late 1980s, as more and more businesses began to use Fax machines, the marketers decided that they could Fax you their advertisements. For anyone in a busy office in the late 1980s, you will remember the piles and piles of office supply advertisements and business printing ads that came pouring out of your Fax machine... making it impossible to get the Fax that you were expecting from your East Coast office.

This problem spawned the original Anti-Junk-Fax law that CAUCE is seeking to amend. In the first major court challenge to that law, a junk fax company called Destination Ventures lost their suit. The 9th Circuit Court of Appeals said that the law was constitutional because the imposition of such high costs and inconvenience onto businesses and consumers made the law a reasonable restriction[25]. By extension, we argue that junk e-mail isn't very different from junk faxes in the way it consumes the resources of others. Spam can and will overwhelm your electronic mail box if it isn't fought. Unless the growth of UCE isn't stopped, over time it will destroy the usefulness and effectiveness of e-mail as a communication tool.

Annoyance Factor

Your e-mail address is not the public domain! It is yours, you paid for it, and you should have control over what it is used for. If you wish to receive tons of unsolicited advertisements, you should be able to. But you shouldn't be forced to suffer the flood unless and until you actually request it. This is the heart of the "Opt In[26]" approach supported by CAUCE.

But what about junk mail makes it so annoying? In part, it's because accessing e-mail for many people is still a bit of a struggle. For example, try as they may, many of the major online services are still hard to connect into. Their software doesn't always configure very easily. After a few calls to customer support, you finally got it installed. So, after being away for a few days, you try to get your e-mail. Of course, you have to keep dialing, dialing, dialing... busy signals. Finally you connect -- only it might be a 9600 baud[27] connection, because all of their 28.8 modems are busy. Still,

you're finally connected and you see that "You've got mail!"

But when you try to retrieve your e-mail, the "System Is Not Responding. Please Try Again Later." After five or ten more minutes of this, you finally get your e-mail to start downloading. You were only out of town for four days; there must be a lot of mail, because it takes you about 10 minutes to get it all downloaded. Once you've retrieved it all, you open it up, and what do you see? Five pornographic web site spams, three letters from some guy named Dave Rhodes and his cousin Christopher Erickson telling you how to make $50,000 in a week, somebody telling you that you're too fat and you need Pyruvate (sprinkled with Blue Green Algae), and two offers to buy stock in a "New Startup Company"...only the broker is a really bad speller and can't decide whether he's selling "stock" or "stork."

Oh, and there was an e-mail from the "Postmaster" telling you that when you tried to "Remove" yourself from a junk e-mail list, the address "Work.At .Home@noreply.org" was of course "Unknown." So after a half hour of delays and frustration, all you've got to show for your efforts is a box full of spam. Is it any wonder people are annoyed?

Ethics

Spam is based on theft of service, fraud and deceit as well as cost shifting to the recipient. The great preponderance of products and services marketed by UCE are of dubious legality. Any business that depends on stealing from its customers, preying on the innocent, and abusing the open standards of the Internet is -- and should be -- doomed to failure.

(Quoted with permission) http://www.cauce.org/about/problem.shtml.

UCE poses a serious threat to ISP's and to Internet users in general. The question remains, however, as to what protections and remedies the law affords in the 6th Judicial Circuit; Kentucky, Tennessee, Ohio, and Michigan. What statutes are there that address UCE? What penalties and remedies are available to Internet users? What case law has developed in the 6th Circuit regarding UCE?

The Laws Within the 6th Circuit; State and Federal

The States located in the 6th Judicial Circuit all have anti-UCE legislation in place with the exception of Kentucky. As of the date of this paper there is no law against UCE in Kentucky of any kind. As for the States with anti-UCE statutes, there are significant similarities. All three States' statutes require spammers to include certain contact information within a UCE. All the statutes require the recipient of UCE or a service provider to have some ties to the State. All the State statutes prohibit certain covert actions by spammers to conceal the address the UCE was sent from. All three States prohibit the sale of software designed to conceal the sender's e-mail address or IP address[28]. Also all the State statutes provide civil remedies for those who receive UCE's in violation of their statute and for ISP's. Michigan actually criminalizes spamming and makes a violation of its statute a misdemeanor.

Michigan and Ohio both provide defenses for spammers. Michigan provides the defenses of "accident" or accidental sending of a UCE and "preexisting business relations" which seems self-explanatory. Ohio also provides "preexisting business relations" as a defense but includes "consent" or agreement to receive the UCE and "forward". "Forward" simply refers to the forwarding of a UCE from a friend. One cannot sue a spammer because his friend forwarded the UCE.

All three States also provide for civil remedies against a spammer who violates that particular statute. However, Michigan's legislation is by far the most severe containing criminal penalties as well as staggering civil remedies. Michigan's statute also allows its Attorney General to bring a civil action against a spammer who violates the Michigan Act.

Michigan

Michigan has one of the most advanced and recently passed anti-UCE statutes of all the 50 states. The Michigan Legislature passed the *Unsolicited Commercial E-mail Protection Act* (UCEPA) on September 1, 2003. This Act is located at MCL §§ 445.2501 through 445.2508 in the Michigan Compiled Law. This Act provides specific guidelines that Spammers must abide by when sending UCE, prohibits certain actions by Spammers, makes violation of the Act a criminal offense, and finally provides a civil remedy for those damaged by Spammers.

The UCEPA requires Spammers to include the term "ADV:" in the subject line of every e-mail[29]. There is little doubt that the legislature saw the opportunity for users to simply filter out all e-mails with such terms in the subject line. It also requires that Spammers include key contact information within the body of the text of the e-mail[30]. Spammers are also required to provide information to the recipient necessary to "opt out" of receipt of any further e-mail[31]. This information must be in print the same size as the rest of the e-mail[32].

The UCEPA prohibits Spammers from using third parties to transmit UCE's without that parties consent[33]

or using a third party to send an e-mail to a recipient who has "opted out" of that Spammer's UCE's[34]. The Act also prohibits Spammers from failing to include the UCE's point of origin information[35]. This would include providing a dead or non-working return address so the recipient could not send a return e-mail. In fact the Act makes it prima facie evidence of a violation of the UCEPA if the recipient can not contact the Spammer through the return e-mail address provided[36]. The Act also prohibits the sale, distribution, or possession of software that allows a Spammer to disguise where the UCE came from[37].

Michigan made Spamming a crime under certain circumstances. MCL § 445.2507 makes it a misdemeanor to violate the UCEPA[38]. A violation of the UCEPA will result in one year's imprisonment or a maximum fine of $10,000.00[39]. Spammers beware because each UCE is a separate violation of the UCEPA[40]. This could quickly add up for those Spammers sending UCE's in bulk quantities. The UCEPA provides a safe harbor for Internet Service Providers (ISP's)[41] that are simply doing their jobs transmitting data for customers[42]. The Act also creates two defenses to allegations of a violation; accident and "preexisting business relations." Accidental transmission is a defense to a charge of a UCEPA violation and so is the existence of a business relationship prior to sending the UCE[43]. "Preexisting business relations" is defined by the Act as "a relationship existing before the receipt of an e-mail formed voluntarily by the recipient with another person by means of an inquiry, application, purchase, or use of a product or service of the person sending the e-mail[44]."

The UCEPA also allows a civil action to be brought by the Attorney General[45], an e-mail service provider (ESP)[46], or persons receiving UCE's[47] that violate the Act. These three classes of plaintiff can receive actual damages incurred or, instead of actual damages, whatever amount would add up to be less; $500 per UCE or $250,000 per day that the violation(s) occur[48]. The Act goes on to provide the prevailing ESP or UCE recipient with actual costs and attorney fees[49]. However it should be noted that the Act requires that the spammer knew or should have known that the recipient or the ESP were residing or located, respectively, in the State of Michigan[50]

Tennessee

The Tennessee Legislature approved its anti-UCE law in 1999 and is therefore the oldest anti-UCE law in the 6th Circuit. It was recently amended in 2003 to delete all references to fax transmissions. Tennessee Code Annotated (TCA) § 47-18-2501 is referred to generally as the *Unsolicited Advertising by Electronic Means* (UAEM) statute. This statute is similar to Michigan's in many ways but its effectiveness is limited to Tennessee spammers. Tennessee businesses are prohibited from sending UCE's unless they contain contact information allowing the recipient to contact the spammer[51] and are required by law to provide that contact information[52]. Tennessee based spammers must respect recipients' requests not to send any more UCE's[53]. It is interesting to note that Tennessee's statute limits its mandates to spammers located within the State of Tennessee.

Tennessee requires all spammers to include the term "ADV:" in the subject line of their UCE's similar to Michigan's statute[54]. However, Tennessee also requires spammers to use the term "ADV: ADLT" in the subject line when adult content is included in a UCE[55]. This would mean, of course, that an advertisement for penis enlargement or sexual enhancements would require the "ADV: ADLT" term in its subject line. The Tennessee statute limits its application to UCE's that are delivered to a Tennessee resident through a Tennessee based ESP or a Tennessee based ESP's equipment that is located in Tennessee[56]. There are prohibitions in Tennessee's statute identical to Michigan's against the sale, distribution, or possession of any software allowing a spammer to disguise where the e-mail was sent from[57].

Tennessee's statute does not criminalize the act of sending UCE's as does Michigan's Act. The Tennessee statute does allow for a civil action against a spammer by an ESP or an individual. The statute allows for actual damages incurred, cost of suit, and loss of profits[58]. However Tennessee's remedies in lieu of actual damages are significantly less than Michigan's. For both an ESP and an individual the statute allows only $10.00 per UCE or $5,000 per day the violation occurs, whichever is less[59]. The statute also provides no cause of action between an individual and an ESP (or a safe harbor) when the ESP simply transmitted UCE's to that person in the course of its business[60].

Ohio

Ohio's statute became effective November 1st, 2002. The statute requires a recipient to have some ties to the State of Ohio[61] similar to the Michigan statute but has no mens rea requirement that the spammer have any knowledge of that recipient's domicile. The Ohio stat-

ute requires that a spammer include their name, address, and e-mail address within the UCE[62]. The statute also mandates that the spammer include language within the UCE informing the recipient that they may "opt out" which must be of the same size font as the entire UCE's font[63].

Similar to the Michigan statute, the Ohio statute provides spammers with defenses against an alleged violation. The statute provides spammers with the defenses of "consent"[64], "preexisting relations"[65], and or "forward"[66]. As in Tennessee and Michigan, ESP's are also given safe harbor in the Ohio statute[67].

Ohio's statutory remedies do not allow actual damages for individuals or ESP's. There is no mention of actual damages anywhere in the Ohio statute. Instead the statutory remedies Ohio allows are "per diem" and "per violation" indemnification, similar to the Michigan and Tennessee statutes. A recipient who receives UCE's in violation of the Ohio statute can sue for $100 per violation (not to exceed $50,000.00), reasonable attorney fees, and court costs[68]. An ESP may bring a civil suit against a spammer for $50.00 per violation, reasonable attorney fees, and court costs[69]. The statute further allows a recipient to obtain an order enjoining any further UCE's from the spammer[70]. However the most unique aspect to Ohio's anti-UCE statute is that it equates the disguise or falsification of a UCE's point of origin as forgery under its statutory code[71].

Kentucky

Kentucky has no statute regarding UCE's. There is no law against UCE's within the State of Kentucky and it is unclear whether there are any bills before its Legislature.

Federal

On December 16, 2003, President Bush signed into law the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (CAN-SPAM Act), which establishes a framework of administrative, civil, and criminal tools to help America's consumers, businesses, and families combat unsolicited commercial e-mail, known as spam[72]. CAN-SPAM became effective on January 1, 2004 and is so new that the United States Code Annotated (USCS) cites to no case s showing Courts' application of the recent law.

Since Congress passed a federal law dealing with an area they are constitutionally granted power over, it would seem that the above description of the States' statutes is for naught. If one remembers their basic Unites States Government class then the concept of "preemption" will come to mind. In *Crosby v. National Foreign Trade Council*[73], the Supreme Court explains the concept of preemption articulately.

> A fundamental principle of the Constitution is that Congress has the power to preempt state law. Art. VI, cl. 2; *Gibbons v. Ogden*, 22 U.S. 1, 9 Wheat. 1, 211, 6 L. Ed. 23 (1824); *Savage v. Jones*, 225 U.S. 501, 533, 56 L. Ed. 1182, 32 S. Ct. 715 (1912); *California v. ARC America Corp.*, 490 U.S. 93, 101, 104 L. Ed. 2d 86, 109 S. Ct. 1661 (1989). Even without an express provision for preemption, we have found that state law must yield to a congressional Act in at least two circumstances. When Congress intends federal law to "occupy the field," state law in that area is preempted. Id. at 100; cf. *United States v. Locke*, 529 U.S. 89, 120 S. Ct. 1135, 146 L. Ed. 2d 69 (2000) (slip op., at 23) (citing Charleston & Western Carolina R. Co. v. Varnville Furniture Co., 237 U.S. 597, 604, 35 S. Ct. 715, 59 L. Ed. 1137 (1915)). And even if Congress has not occupied the field, state law is naturally preempted to the extent of any conflict with a federal statute. *Hines v. Davidowitz*, 312 U.S. 52, 66-67, 85 L. Ed. 581, 61 S. Ct. 399 (1941); ARC America Corp., supra, at 100-101; Locke, supra, at (slip op., at 17). We will find preemption where it is impossible for a private party to comply with both state and federal law, see, e.g., *Florida Lime & Avocado Growers, Inc. v. Paul*, 373 U.S. 132, 142-143, 10 L. Ed. 2d 248, 83 S. Ct. 1210 (1963), and where "under the circumstances of [a] particular case, [the challenged state law] stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Hines, supra*, at 67.

The above quote makes it clear that CAN-SPAM preempts state law because UCE's clearly involve commerce and Congress has the power regulate commerce according to the Constitution[74]. In addition, CAN-SPAM expressly states that it supersedes state law[75]. If this is the case what does CAN-SPAM do for 6th Circuit state residents that their States' law does not and what, if anything, does CAN-SPAM not do that the States' laws did?

What Does CAN-SPAM Say?

15 USCS § 7704: What Rules Must UCE's **Abide By**

CAN-SPAM lays out certain requirements that a spammer must abide by when sending a UCE. One requirement, similar to the States', is that the header information can not be "materially false or misleading[76]."

Header information is materially false or misleading[77] if it is obtained by means of false or fraudulent pretenses[78] and if it fails to identify the computer it was actually sent from[79]. CAN-SPAM also prohibits the use of false or misleading subject lines used to persuade a recipient to open a UCE[80]. CAN-SPAM also requires that spammers include means by which a recipient can "opt out" of receiving any further UCE's from them[81]. One should think about Brian Miller's illustration above of the time it takes to "opt out" of each of these e-mails. The Act also prohibits a spammer from sending an "opt out" recipient any more UCE's[82].

Spammers must include certain information within UCE's. CAN-SPAM requires spammers to include a notice that the message is an advertisement, information that the recipient can "opt out" of any more UCE's, and a valid return postal address[83]. CAN-SPAM also states that if a person has given prior affirmative consent then no notice of advertisement need be included in the UCE[84]. This is differs from Ohio's "consent" defense in that CAN-SPAM simply waives an informational requirement whereas Ohio provided a spammer with a defense against allegations of a violation.

CAN-SPAM makes it an aggravation of violating the Act if a spammer sends UCE's that violate CAN-SPAM toe-mail addresses it obtained by address harvesting, as discussed in part one of this paper, or dictionary attacks[85]. CAN-SPAM specifically describes these two types of software programs[86]. The Act also prohibits covert attempts at hiding or disguising a UCE's point of origin by using an innocent third party or by using anonymous e-mail user accounts[87].

CAN-SPAM makes it a criminal violation to send UCE, which contains material that depicts sexually explicit conduct[88] without including some notice in the subject line of the adult content[89]. This is similar to the "ADV: ADLT" requirement that Tennessee's statute required. The Act empowers the Federal Trade Commission (FTC) to issue regulations implementing the provisions of CAN-SPAM[90]. There is also a requirement that no later than April 16, 2004, or 120 days after the enactment of CAN-SPAM, the FTC and the Attorney General shall prescribe what mark or term should be used for this purpose[91]. Interestingly, the Act expressly forbids the FTC from prescribing a mark or term that would alert recipients that the UCE is in fact an advertisement[92]. This would forbid the requirement of the term "ADV:" in a header, which both the Tennessee and Michigan statutes required.

CAN-SPAM also prohibits trades and businesses from knowingly promoting their goods or services through UCE's that violate the Act[93]. This extends the reach of the statute beyond the spammer to the entity or person ultimately responsible for the UCE.

Enforcement: Who and How?

CAN-SPAM states that the FTC shall enforce the Act and that a violation of CAN-SPAM is an unfair or deceptive act or practice[94] according to the Federal Trade Commission Act. CAN-SPAM also unleashes a dozen other federal agencies to enforce compliance with the Act[95]. These other agencies, however, must comply with FTC rules and regulations in enforcing the Act's provisions. The Act also states that the FTC has all the powers, rights, tools, and authority granted to it under the Federal Trade Commission Act in enforcing CAN-SPAM[96]. The FTC can obtain injunctive relief to enjoin spammers from continuing to violate CAN-SPAM. However, the FTC is not required to prove the alleged violators' mens rea when the FTC or the Federal Communications Commission (FCC) requests a court to grant an injunction or an order to cease and desist[97].

"This is just a bunch of mumbo jumbo," you say " the FTC will never implement this plan." The FTC website announces that:

> **FTC Announces First Can-Spam Act Cases, April 29, 2004**
>
> The FTC has cracked down on two spam operations that have clogged the Internet with millions of deceptive messages and violated federal laws. A complaint targeting Detroit-based Phoenix Avatar was developed in a joint investigation with the U.S. Attorney's Office in Detroit and the U.S. Postal Inspection Service. At the request of the FTC, a U.S. District Court judge has barred the illegal spamming and frozen the defendants' assets. Federal criminal authorities yesterday executed a criminal search warrant and are in the process of arresting four principals in that case. In the second case, the FTC filed a legal action against Global Web Promotions, a spam enterprise that operates out of Australia and New Zealand.
>
> Both operations have been identified by the anti-spam organization Spamhaus as among the largest spammers in the world. Consumers forward unwanted spam e-mail to the FTC, which maintains it in a database. Since January 1, 2004, consumers have complained to the FTC about 490,000 spam messages linked to Phoenix Avatar and 399,000 messages for Global Web Promotions.
>
> (Quoted without permission) the FTC website; http://www.ftc.gov/opa/2004/04/040429canspam.htm.

The FTC filed a four count complaint[98] against several Defendants, Phoenix Avatar LLC d/b/a Avatar Nutrition, DLJ, LLC, Daniel J. Lin, Mark M. Sadek, James Lin, and Christopher M. Chung d/b/a AIT Herbal Marketing alleging, among other things, violations of CAN-SPAM. The Defendants sent UCE's regarding fraudulent diet products to hundreds of thousands of recipients on a daily basis. These recipients in turn forwarded the messages to the FTC. Several of the Defendants had ties to Michigan. It is unclear from the complaint why the suit was brought in Illinois. The complaint generally alleges violations of the above mentioned requirements that CAN-SPAM lays out for UCE's. There is mention in the complaint of the aggravating factor that the companies used third party return addresses to disguise their true point of origin. This could allow for treble damages if the FTC pursues that remedy.

In the second case the FTC is pursuing, the FTC has filed a six-count complaint against several Defendants, Global Web Promotions Pty. Ltd, Michael John Anthony VanEssen, and Lance Thomas Atkinson. This company, located in Australia, has sent UCE's to thousands promising dietary and anti-aging secrets. The complaint cites law from the Federal Trade Commission Act establishing jurisdiction, but it is unclear how that law applies to an Australian company or individuals. It is clear that whatever assets the company has in the United States are now frozen. Whatever the outcome is regarding these two cases it is clear that the FTC takes this Act seriously.

What CAN-SPAM Allows States To Do On Behalf Of Their Residents?

CAN-SPAM allows a state Attorney General, Official, or Agency to bring a civil suit in the interest of one of its citizens for a violation of CAN-SPAM[99]. It should be noted that this is for a violation of CAN-SPAM, not that particular States' law. If the proper state authority does bring suit in "parens patriae"[100] they can obtain relief in the form of an injunction or monetary damages[101]. The statute allows injunctive relief to be obtained without showing the alleged violator's mens rea[102] same as for the FTC or FCC. However the damages available under CAN-SPAM are either actual monetary losses suffered or those provided for in the Act itself[103].

The damages that CAN-SPAM allows "state-initiated" suits, as an alternative to actual monetary damages, are simple; the number of CAN-SPAM violations multiplied by a monetary amount, the maximum of which is $250.00, with a total that can not exceed $2 million[104]. However, the court may disregard the $2 million limit and award up to triple damages if the CAN-SPAM violator did so willingly, knowingly, or used address harvesters or dictionary attacks in obtaining the addresses it spammed[105]. The "state-initiated" suit is also allowed costs and attorney fees. "State-initiated" suits require the state official bringing the suit to prove the defendant acted with actual knowledge or knowledge fairly implied on the basis of objective circumstances in order to recover any monetary damages[106].

Before bringing suit against a spammer a "state-initiated" suit must give notice to the FTC and all other federal agencies that CAN-SPAM has activated to enforce its provisions[107]. If the FTC or any of the other agencies has a suit pending against the alleged spammer then the "state-initiated" suit is forbidden[108].

Internet Service Providers? What About Them?

The damages allowed ISP's are almost identical to those allowed "state-initiated" suits brought by a state official on behalf of a resident. ISP's are allowed injunctive relief, actual monetary damages, or statutory damages similar in setup to the state resident's damages[109]. ISP's statutory damages are calculated according to the type of violation. If the spammer violates the informational requirements laid out by the Act then the ISP can get a monetary amount equal to the number of CAN-SPAM violations multiplied by up to $100.00[110]. Any other CAN-SPAM violation and the ISP can get monetary damages equal to the number of violations multiplied by up to $25.00[111]. Attorney's fees and costs to bring the suit may be allowed. The same aggravating factors that give state residents triple damages also give ISP's triple damages[112].

Do Not E-Mail Registry

CAN-SPAM also mandates that by June 16, 2004 the FTC shall have a report outlining a plan to implement a National "Do Not E-Mail" Registry similar to the "Do Not Call List[113]." The FTC also must determine how the registry will work and any problems that it sees in its implementation[114]. It is unclear how close the FTC is to this task. They have issued a Request for Information on their website asking for technical assistance in drafting the plan[115].

Analysis of Federal v. State Protections and Remedies

It becomes apparent after one peruses through CAN-SPAM that private suits by state residents are no longer permitted. In the 6th Circuit one must now go to their State's Attorney General's Office to initiate a suit against a spammer. The Attorney General's Office in every state is overworked already without adding more to its plate. CAN-SPAM doubles the pressure on State Attorney Generals' Offices by making that the only way a private citizen can obtain a remedy.

Michigan's wonderfully drafted UCEPA is no longer effective against would be spammers. Michigan's law provided serious penalties and civil damage remedies and in so doing provided powerful deterrence against UCE's. Three months after it went into effect CAN-SPAM effectively killed Michigan's UCEPA by preemption. On January 1st, 2004 CAN-SPAM "hamstrung" all state laws by doing away with private citizen actions against spammers within the 6th Circuit.

Congress thought it was declaring open season on spammers by unleashing more than a dozen federal agencies to enforce CAN-SPAM. However, a dozen or so agencies does not compare to millions of state citizens with the power to initiate their own suits against spammers. Private suits would show that spammers have no place to hide. However it can be argued that the FTC and other agencies have far more power than a private citizen does against a spammer. They have abilities to cooperate with federal law enforcement to seize property or freeze assets as well as other possible methods of investigation.

CAN-SPAM prohibits any regulation requiring a spammer to designate their UCE's as advertisements. The Michigan, Tennessee, and Ohio statutes all required the term "ADV:" to be included in the subject line of the UCE. CAN-SPAM makes it harder for Internet users to filter out unwanted UCE's while the state laws made it quite simple. CAN-SPAM also makes it criminal to send sexually explicit material by UCE without some designation of such in the message's header. It is still unclear what universal term the FTC will choose to designate adult content in UCE's.

CAN-SPAM's requirements for UCE's are far less stringent than the state laws. It seems as though spammers had some input in the drafting of the federal statutes. It would also appear that Congress is trying to regulate UCE's instead of outright banning them. As long as spammers comply with certain set requirements then its business as usual. The problem still remains however that Spam or UCE's are still allowed. Hundreds of companies have formed and put up a shingle on the Internet touting themselves as experts in "CAN-SPAM compliance." CAN-SPAM's result seems to be that spammers simply have to spend a little more to send UCE's.

The States' Laws in the 6th Circuit were much better at deterring spammers than CAN-SPAM. They provided strict requirements, severe penalties (especially Michigan), and private suits. CAN-SPAM seems to be a watered down version of what the states had already set up. If CAN-SPAM is to be effective it needs to give companies like an accounting firm, a law firm, or other professional business the power to initiate a suit against a spammer who sends UCE's to all its personnel making it incur time and money costs in dealing with this problem. Instead these businesses must fill out a form, send it to their State's overworked Attorney General's Office, and then wait for a reply while the Attorney General processes the complaint. Not very pro-active in dealing with spammers.

The Jurisdiction Problem

The FTC must account for the growing number of offshore businesses spamming US residents. Many businesses either move offshore or use ESP's located offshore in an attempt at hiding their country of origin. Jurisdiction is a funny thing on the Internet and spammers know this. The recent case of FTC v. Global Web Promotions [116] will illustrate what happens in this situation, as the Defendant in that case is located in Australia. According to the FTC website Australian authorities cooperated with the FTC by handing over the spammers.

The leading case on Internet jurisdiction is *Zippo Mfg. Co. v. Zippo DOT Com*[117]. *Zippo* explains how a court will analyze a company's contacts with the forum in determining jurisdiction and venue. *Zippo* states:

> The Internet makes it possible to conduct business throughout the world entirely from a desktop. With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages. The cases are scant. Nevertheless, our review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well-developed personal jurisdiction principles. At one end of the

> spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. E.g. *Compuserve, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996). At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. E.g. *Bensusan Restaurant Corp., v. King*, 937 F. Supp. 295 (S.D.N.Y. 1996). The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. E.g. *Maritz, Inc. v. Cybergold, Inc.,* 947 F. Supp. 1328, 1996 U.S. Dist. LEXIS 14978 (E.D.Mo. 1996).

Zippo at 1123-1124. Thus, in causes of action that arise from Internet contacts, courts will analyze defendants doing business on the Internet according to a sliding scale.

Although the above quote discusses websites, UCE's can be seen as active contacts in that they are sent to recipients. *Zippo* could be interpreted as extending jurisdiction over an out of state or an out of country defendant because of their active and aggressive contacts with US citizens. Sending UCE's is quite active contact and could be enough to qualify for personal jurisdiction.

The protections and remedies allowed residents of the 6th Circuit are inadequate in light of current UCE problems. Statutory law in the 6th Circuit was seriously compromised by the enactment of CAN-SPAM. CAN-SPAM has empowered government and taken power away from private citizens. CAN-SPAM has seriously compromised 6th Circuit residents' remedies and protections against UCE's and spammers. Suits by individuals are not allowed unless that person goes to their State's Attorney General's Office and files a formal complaint. UCE requirements are not as stringent as the State laws were allowing spammers more leeway in sending UCE's.

CAN-SPAM seems to merely regulate UCE's not ban them. Services offering CAN-SPAM compliance are popping up all over the Internet declaring that they can help spammers beat CAN-SPAM. It seems that all the Act did was make it a little more expensive for spammers to send UCE.

Michigan was the most seriously affected State of the 6th Circuit by CAN-SPAM's preemption. The UCEPA was a well-drafted Act, which made it criminal to send UCE's that violated the Act. It also provided a civil remedy for Michigan residents and ISP's who received or were injured by UCE's in violation of the Act. It also allowed its Attorney General to bring actions against spammers. The penalties laid out in UCEPA were quite substantial and were an excellent deterrent against UCE's. Now UCEPA is laid to rest as CAN-SPAM moves in taking over with less effectiveness against spammers and more liberal requirements for UCE's.

Overall the protections and remedies available in the 6th Circuit against UCE's were seriously undermined by CAN-SPAM. However with the advent of the two new FTC cases being brought in a Federal Court in Illinois perhaps spammers will see what punishments await them if they send UCE's. Ultimately CAN-SPAM's effectiveness now lies in its enforcement by the FTC. Just how aggressive they will enforce this Act remains to be seen.

Endnotes

1. Term used to refer to those who send UCE or Spam.
2. A list of e-mail addresses identified by a single name, such as *mail-list@sandybay.com*. When an e-mail message is sent to the mailing list name, it is automatically forwarded to all the addresses in the list. http://www.webopedia.com/TERM/M/mailing_list.html
3. An on-line discussion group. On the Internet, there are literally thousands of newsgroups covering every conceivable interest. http://www.webopedia.com/TERM/N/newsgroup.html
4. definitions from http://spamlinks.openrbl.org/faqs.htm
5. This section was developed from Uri Raz's post entitled "How Do Spammers Get People's E-mail Address?" at http://www.faqs.org/faqs/net-abuse-faq/harvest/ however this article has been cited by so many other authors it is unclear exactly who wrote it. It does sum up the many ways spammers get e-mail addresses quite well.
6. A worldwide bulletin board system that can be accessed through the Internet or through many online services. The USENET contains more than 14,000 forums, called *newsgroups*, which cover every imaginable interest group. It is used daily by millions of people around the world. http://whatis.techtarget.com/definition/0,,sid9_gci213807,00.html
7. Munge refers to text inserted into an e-mail address to render it invalid and thus useless to spammers. For example, the address `jrandom@hacker.org' might be transformed to `jrandom@NOSPAM.hacker.org'. Adding spamblock to an address is often referred to as "munging it". This evasion tactic depends on the fact that most spammers collect names with some sort of **address harvester** on volumes too high to demunge by hand, but individual humans reading an e-mail message can readily spot and remove a spamblock in the "From" address. http://developer.syndetic.org/query_jargon.pl?term=mung
8. Short for **H***yper***T***ext* **M***arkup* **L***anguage,* the authoring language or code used to create documents on the World Wide Web. http://archive.ncsa.uiuc.edu/General/Internet/WWW/

HTMLPrimerAll.html

[9] Databases containing e-mail addresses, telephone numbers, and postal addresses of Internet users. You can search the Internet White Pages to find information about particular users including e-mail addresses.

[10] http://www.bigfoot.com/. Bigfoot Communications offers a service where you type in a person's name and they search the web for any and all possible e-mail addresses registered or connected to that person in some way.

[11] A program that allows a user to find, view, hear, and interact with material on the World Wide Web. Netscape Navigator and Microsoft Internet Explorer are examples of popular browsers. http://www.protecteverychild.org/html/glossary_of_commonly_used_term.php

[12] A very common method of moving files between two Internet sites. FTP is a way to login to another Internet site for the purposes of retrieving and/or sending files. There are many Internet sites that have established publicly accessible repositories of material that can be obtained using FTP, by logging in using the account name "anonymous", thus these sites are called "anonymous ftp servers". FTP was invented and in wide use long before the advent of the World Wide Web and originally was always used from a text-only interface. http://www.u2networks.com/library/glossary_e.htm

[13] An example is when you sign in to your e-mail account and then check the box stating "Remember my ID on this computer" so that the next time you access your e-mail you don't have to type in any password or ID to log-in.

[14] An open-source HTML compatible programming language or code that is used by many web site designers to create dynamic content on their sites. http://grunge.cs.tu-berlin.de/~tolk/vmlanguages.html

[15] Small Java programs used on Web pages to operate animation, calculators, and other tasks. http://www.adn.com/adn/help2/online_mk/glossary.html

[16] Visual Basic — a popular Microsoft programming language used by accounting software vendors to build graphical client application interfaces.

[17] A Web Bug is a graphics on a Web page or in an E-mail message that is designed to monitor whom is reading the Web page or E-mail message. Web Bugs are often invisible because they are typically only 1-by-1 pixel in size. They are represented as HTML IMG (IMG = image) tags. http://www.eff.org/Privacy/Marketing/web_bug.html

[18] Many if not most Web sites use scripts (little programs embedded in the web page data) for many purposes, usually benign and often helpful. These programs perform a variety of operations but are usually used for animations. http://www.popupcop.com/help/glossary.html

[19] This virus was a Word 97 macro virus with a deadly capability. It had the ability to spread itself very fast using e-mail. When the document infected by Melissa virus was opened for the first time, the virus checked whether the user's computer was installed with MS Outlook. If it found Outlook then the virus would send e-mail to 50 addresses in the user's Outlook address book. The e-mail sent by the virus would contain the subject "Important Message From {user name}". The body of the e-mail would contain "Here is that document you asked for . . . don't show anyone else :-)". The virus would attach the infected document to the message. This virus spread very fast because of this method. http://www.pspl.com/virus_info/w97m/melissa.htm

[20] This is the unique name that identifies an Internet site. Domain Names always have at least two parts, which are separated by dots (for instance "microsoft.com"). The part on the left is specific whereas the part on the right is more general. http://www.hostapproval.com/hosting_terminology_d.html

[21] Anyone can go to http://www.networksolutions.com/en_US/whois/index.jhtml and perform a "WhoIs" Search. This search allows one to find out the identity of the owner of a domain name and their contact information.

[22] The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz). http://www.tophosts.com/articles/?1226.html

[23] See website at http://www.cauce.org/index.phtml

[24] The **Coase Theorem** states that if private parties can bargain without cost over the allocation of resources, then they will be able to resolve an externality, resulting in the efficient allocation of resources. However, if the interested parties cannot reach or enforce a bargain, or if the bargaining process incurs a transaction cost, then the externality will not be resolved and will require the intervention of another party, the government. http://www.informationgenius.com/encyclopedia/c/co/coase_theorem.html

[25] *Destination Ventures v. FCC*, 46 F.3d 54 (9th Cir. 1995).

[26] There are two schools of thought. "Opt In," means that as default no one gets Spam until they physically choose to. "Opt Out" means that everyone gets Spam until they physically choose not to.

[27] In common usage the baud rate of a modem is how many bits it can send or receive per second. www.netbenefit.com/support_glossary.html

[28] An IP address is a string of numbers consisting of four sets of numbers, each separated by periods. Each IP address uniquely identifies a certain computer on the Internet. An example of an IP address is 123.123.4.5. http://encyclopedia.thefreedictionary.com/IP%20number

[29] MCL §445.2503(a)

[30] MCL §445.2503(b)

[31] MCL §445.2503(c) and (d)

[32] Id.

[33] MCL §445.2504(1)(a)

[34] MCL §445.2504(2)

[35] MCL §445.2504(1)(c)

[36] MCL § 445.2507(5)

[37] MCL § 445.2505

[38] MCL §445.2507(1)

[39] Id.

[40] MCL §445.2507(3)

[41] Internet Service Providers are organization or companies that provides Internet connectivity. Access services provided by ISPs might include web-hosting, email, VoIP (voice over IP), and support for many other applications. Examples would be Comcast and AOL. http://www.definethat.com/define/?id=103

[42] MCL § 445.2507(4)

[43] MCL § 445.2507(6)

[44] MCL § 445.2502(g)

[45] MCL § 445.2508(3)

[46] MCL § 445.2508(2); MCL § 445.2502 defines e-mail service provider as a person that is an intermediary in the transmission of e-mail or provides, to end users of e-mail service, the ability to send and receive e-mail.

[47] MCL § 445.2508(1)

[48] MCL § 445.2508(4)

[49] MCL § 445.2508(5)

[50] MCL § 445.2503

[51] TCA § 47-18-2501(a)

[52] TCA § 47-18-2501(d)

[53] TCA § 47-18-2501(c)

[54] TCA § 47-18-2501(e)

[55] Id.

[56] TCA § 47-18-2501(f)

[57] TCA § 47-18-2501(g)

[58] TCA § 47-18-2501(i)(1)

[59] TCA § 47-18-2501(i)(2) and (3)

[60] TCA § 47-18-2501(i)(2)

[61] ORC Ann. 2307.64(A)(11) defines "recipient" as a person who receives an electronic mail advertisement at any one of the following receiving addresses:
(a) A receiving address furnished by an electronic mail service provider that bills for furnishing and maintaining that receiving address to a mailing address within this state;
(b) A receiving address ordinarily accessed from a computer located within this state;
(c) A receiving address ordinarily accessed by a person domiciled within this state;
(d) Any other receiving address with respect to which the obligations imposed by this section can be imposed consistent with the United States Constitution.

[62] ORC Ann. 2307.64(B)(1)(a)

[63] ORC Ann. 2307.64(B)(1)(b)

[64] ORC Ann. 2307.64(B)(3)(b) consent is defined as recipient consents or agrees as a condition of service to receive e-mail.

[65] ORC Ann. 2307.64(B)(3)(a); According to ORC Ann. 2307.64(A)(9) "preexisting business relations" is defined as "there was a business transaction between the initiator and the recipient of a commercial electronic mail message during the five-year period preceding the receipt of that message. A pre-existing business relationship includes a transaction involving the free provision of information, goods, or services requested by the recipient. A pre-existing business relationship does not exist after a recipient requests to be removed from the distribution lists of an initiator pursuant to division (B) of this section and a reasonable amount of time has expired since that request.
[66] ORC Ann. 2307.64(B)(3)(c); "forward" results when the recipient receives the electronic mail advertisement because another recipient forwarded the advertisement to that recipient via an internet web site or another recipient made a direct referral of that recipient to receive the advertisement.
[67] ORC Ann. 2307.64(D)
[68] ORC Ann. 2307.64(E)

[69] ORC Ann. 2307.64(F)

[70] ORC Ann. 2307.64(G)

[71] ORC Ann. 2307.64(H); According to ORC Ann. 2913.31(C)(1)(b) ". . . forgery is a felony of the fifth degree" in Ohio.

[72] The Whitehouse website; http://www.whitehouse.gov/news/releases/2003/12/20031216-4.html

[73] 530 U.S. 363 (2000).

[74] United States Constitution Art. I, § 8, The Congress shall have power to . . . regulate commerce with foreign nations, and **among the several states**, and with the Indian tribes;

[75] 15 USCS §7707(b)

[76] 15 USCS §7704(a)(1)

[77] According to 15 USCS §7704(a)(6) the term "materially", when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

[78] 15 USCS §7704(a)(1)(A)

[79] 15 USCS §7704(a)(1)(C)

[80] 15 USCS §7704(a)(2)

[81] 15 USCS §7704(a)(3)

[82] 15 USCS 7704(a)(4)

[83] 15 USCS 7704(a)(5)(A)

[84] 15 USCS 7704(a)(5)(B)

[85] A dictionary attack refers to a software program that randomly generates e-mail addresses. This program is capable of processing thousands upon thousands of randomly generated e-mail addresses within an hour with the hope of getting a certain percentage of those guesses right. The addresses that aren't correct simply come back to the sender as "Mail Delivery Failure".

[86] 15 USCS §7704(b)(1)(A)(i) and (ii)

[87] 15 USCS §7704(b)(2) and (3)

[88] According to 18 USCS §2256, "sexually explicit conduct" means—

(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;
(ii) graphic or lascivious simulated;

(I) bestiality;
(II) masturbation; or
(III) sadistic or masochistic abuse; or

(iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

[89] 15 USCS §7704(d)(5)

[90] 15 USCS §7711(a)

[91] 15 USCS §7704(d)(3)

[92] 15 USCS §7711(b)

[93] 15 USCS §7705(a)

[94] 15 USCS §7706(a)

[95] 15 USCS §7706(b)

[96] 15 USCS §7706(d)

[97] 15 USCS §7706(e)

[98] A copy of the complaint can be obtained from http://www.ftc.gov/os/caselist/0423084/0423084.htm

[99] 15 USCS §7706(f)(1)

[100] Latin for "parent of his country." Used when the government acts on behalf of one of its domiciles or residents.

[101] 15 USCS § 7706(f)(1)

[102] 15 USCS § 7706(f)(2); "mens rea" quite simply means the person's mental state when they did the violated action.

[103] 15 USCS § 7706(f)(1)

[104] 15 USCS § 7706(f)(3)

[105] 15 USCS § 7706(f)(3)(C)

[106] 15 USCS § 7706(f)(9)

[107] 15 USCS § 7706(f)(5)

[108] 15 USCS § 7706(f)(8)

[109] 15 USCS § 7706(g)

[110] 15 USCS § 7706(g)(3)(A)

[111] Id.

[112] 15 USCS § 7706(g)(3)(C)

[113] 15 USCS § 7708(a)

[114] Id.

[115] http://www.ftc.gov/ftc/oed/fmo/procure/040224donotemailrfi.pdf

[116] N.D. Ill., Case #: 04C 3022, Judge Aspen

[117] 952 F. Supp. 1119 (W.D. Penn. 1997).

You are invited to

State Bar of Michigan Computer Law Section's Annual Spring Networking Event

Join us for a *Happy Hour* at The Hard Rock Café

May 19, 2005, 5:30 - 7:30 p.m. 45 Monroe St., Detroit, MI 48226

You'll enjoy:

Hot and cold appetizers
Raffle for Hard Rock merchandise
Free Drinks*
Great networking opportunities

Featuring a discussion of the CAN SPAM Act by Dante Benedettini of Berry Moorman

* Registrants receive two free drink tickets as well as free unlimited soda, coffee, and hot or iced tea.

Deadline for registration is May 10, 2005
To register for this event, complete the form below and send with a check or credit card info to the State Bar of Michigan, Attn: Seminar Registration, 306 Townsend St., Lansing, MI 48933, or fax (only if paying with credit card) to (517) 346-6365. Payment must be received before your place will be reserved.

If you have any questions, contact Anthony Targan at targana@dteenergy.com.

Name: _____ P#: P_____

Company:_____

Address:_____

I am a: Section Member	☐ $15	Check enclosed	☐
Section Non-member	☐ $25	VISA	☐
Student	☐ $10	MasterCard	☐
		American Express	☐

I'd like to join the Computer Law Section today and pay the Member's fee for this event:
Section Dues $25 + Event Fee $15 = ☐ $40

If paying by credit card complete the following:
Print name as it appears on card: _____
Credit card #: _____ Expiration Date _____

Amount to be charged: $_____ Signature:_____

State Bar of Michigan
Michael Franck Building
306 Townsend Street
Lansing, MI 48933