Volume IV - Article 2

Forgery in Cyberspace: The Spoof could be on you!

Stephanie Austria*

Spring 2004

Preface

Spoofing is one of the newest forms of cyber-attack, a technological methodology adapted to mask the identity of spammers who have faced hostile reaction in response to bulk, unsolicited, electronic mail messages.[1] Sending Spam, however, is no longer the only reason for deception, as crackers have taken pleasure in the challenge of manipulating computer systems and, additionally, find recreational enjoyment in doing so. In this legal Note, the author's intent is to show that criminal, rather than civil liability is the best way to effectively deter and punish the spoofer. The injury that results when a computer system's technological safety measures fail to adequately safeguard the system affects not only the owner of the hijacked e-mail address, but also the Internet Service Provider, and the Network as a whole. Current Anti-Spam Legislation is arguably ineffective at targeting these particular types of malicious attacks, and a different legal approach is suggested.

This Note will examine Source Address Spoofing, the newest cyber crime, and provide a technological explanation as to how the act of spoofing is perpetrated, as a means of demonstrating criminal intent. As such, civil penalties are not enough. The practice has been referred to as "aggravated spam," spam being an area of great concern in Internet regulation already. It is argued, however, that the focus of legislation should not be on spoofing as an aggravated form of spam, where spam, in fact, embodies first amendment protection as a form of free speech. To so reason supports the imposition of monetary fines as adequate. The focus, rather, should be on the actual e-mail and the Internet itself as an extension of writings and telecommunications, whereby forging the origin of an e-mail address in "cyberspace" constitutes forgery in the same way as is currently prohibited in "real space."

Current legislation is pending in a majority of States to specifically regulate the use of spam. Accordingly, current anti-spam legislation, imposing civil liability, will be analyzed to determine whether it is the right approach for targeting this more heinous type of cyber attack. A stronger deterrent, with penal repercussions, is critical. Using technical explanation, a parallel will be drawn between cyberspace and real space to illustrate why current anti-spam legislation will be ineffective as currently proposed. In support of the argument for criminal liability, current criminal procedures that have been in place for decades, which prohibit misrepresentations by mail in real space, will be applied to cyberspace to show that it is applicable in this new domain as well.

Traditionally, technology has been a vehicle for advancing the goals of society and for effecting social change.[2] However, technology can also be just as easily used to circumvent the law, where the perpetrator effectively has the ability to commit a wrong, and then shield him or herself from liability through technological manipulation. As digital communicative capabilities are increasing in proportion to technological advancement, so too are the abilities to apply that technological knowledge to efforts that may ultimately thwart attempts to keep the Internet honest. While discouraging technological advancement should not be the ultimate goal of any legislation, prohibiting an illegitimate use of technology should be. Legislation generally cannot be responsive to rapid technological changes. Laws that address a problem in its earliest stages, for example, often become obsolete as technology evolves to circumvent the law, or counterproductive as the law discourages the evolution of technological solutions to a problem.

I. The Matrix of the Internet

The Internet is not a single network, but rather a worldwide matrix of hundreds of thousands of networks.[3] When a user transmits a message, the data within that message is divided into “packets”[4] which are routed separately through the networks of the Internet. An e-mail message is divided into two parts: The header, which contains information regarding the sender and the recipient, and the body, which contains the actual text message.[5] Each packet, in fact, is preceded by its own header.[6]

An e-mail address consists of three parts: The User ID, the Domain Name, and the Domain Name Suffix.[7] Nameservers translate Domain Names (including the suffix) into IP Addresses, which consist of numbers that are readable and understandable by the Internet Protocol.[8] The Root Nameservers carry the fundamental part of the transmission, which entails locating Nameservers for the Top Level Domain Suffices.[9] Hundreds of thousands of Nameservers for the various domains handle the rest.[10] Thus, every domain has at least two independent name servers.[11] Massive databases list the matches between each Domain Name and its correlating IP Address.[12]

Internet Protocol is the set of technological standards and specifications that enable the routing of information across networks, so that e-mail messages can be successfully delivered and received.[13] Internet Protocol delineates how the data contained within an e-mail message is divided into “packets,” which are each coded with the IP Address translation.[14] A particular message is comprised of multiple packets, which must be reassembled once they arrive separately at their destination. A second protocol handles this reassembly process.[15]

When an e-mail message is transmitted from one e-mail address to another, the packets generally pass through at least four computers. From the sender’s computer, the packets travel to the mail server computer of the sender’s local Internet Service Provider (“ISP”), or intranet if the message originates from within an organization.[16] The “ISP” computer may then send the packets through a series of other ISPs, each constituting a

"node" in the chain of destination, until arriving at the mail server of the recipient's ISP.[17] The disassembled message remains there until the intended recipient retrieves it onto his or her own computer.[18] The Internet Protocol handles the routing and ties together the whole chain, enabling the data packets to travel through the Internet.[19]

Every computer on the Internet has a unique numerical address, called an Internet Protocol or IP address, which is associated with a more readily recognizable domain name. As the e-mail message travels from sender to recipient, each computer transmitting the message attaches identifying data to the "received field" in the header.[20] The information serves as a kind of electronic postmark for the handling of the message. Ideally, the computers on the network will only accept the packets that are addressed to them,[21] and this is how the e-mail message ultimately "finds" its proper destination. It is possible for a sender to alter (or "spoof") the header information by misidentifying either the computer from which the message originated or other computers along the transmission path.

Source Address Spoofing Defined[22]

A spoofer, in Internet terms, is defined generally as the "cracker"[23] who alters, or "forges," an e-mail address, pretending to originate a message from a different source address than that which he or she truly has. There are many ways a cracker may do this, and there are many types of attacks.[24] The attacker may do this to gain access to a secured site that would accept the "hijacked" address as one of few permissible addresses, or more maliciously, the reason may be to hide the source of any type of attack.[25] "Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords)."[26] Furthermore, the spoofer is sly. He or she may send an e-mail to the victims' accounts claiming to be from a system administrator, and request users to change their passwords to a specified string, threatening to suspend their account if they do not comply. Similarly, they might send an e-mail claiming to be from a person in authority, and request users to send them a copy of a password file or other sensitive information.[27]

How the cracker is able to commit this act:

Spoof attacks occur at the Protocol layer level.[28] When the spoofer's goal is to either gain access to a secured site[29] or to mask his or her true identity, he or she may hijack an unsuspecting victim's address by falsifying the message's routing information so that it appears to have come from the victim's account instead of his or her own.[30] He or she may do so through the use of "sniffers." Since information intended for a specific computer must pass through any number of other computers while in transit, the data essentially becomes fair game, and sniffers may be used to essentially capture the information en route to its destination.[31] Sniffer software can be programmed to select data intended for any or every computer.[32] Thus, the spoofer can use the recipient's address, which is found in the header, and configure his or her own machine to emulate the recipient's machine.[33] When information comes along the network that is intended for the true recipient, the spoofer can receive it instead. In this way, the spoofer is able to

gain entry into those sites to which the recipient had access, and thus has the ability to now steal passwords, credit card information, and other personal information, and use that information for any number of illegitimate purposes. Additionally, the spoofer can also automatically send a packet back to the sender, which makes the sender believe that its message was properly received.[34]

The spoofer may also alter the original e-mail and then relay it on to the intended recipient,[35] or he or she can change the message in its entirety, and send it to a different recipient or recipients altogether.[36] If and when the recipient responds, that message will be routed back to the original sender, not to the spoofer.[37] The spoofer, however, will need to sniff the response off the network for the attack to go unnoticed.[38] Conversely, when the spoofing involves unsolicited bulk e-mail, the attacker will choose not to sniff the responses off the network, thereby remaining unacquainted with the effects of his or her attacks. These hostile reactions have been the cause for spammers to mask their identities initially.

The victim and the injuries involved

The victim of a spoof attack is often unaware that he or she has been violated. Moreover, he or she is likely unaware that his or her address has been hijacked for the purpose of being the perceived sender of an e-mail message, or worse yet, bulk mail that may involve thousands of unsolicited e-mail messages.[39] Additionally, spoofing victims are often then inundated with thousands of “bounced-back” e-mails from bad addresses, but even worse, an inevitable multitude of angry recipients send their own messages, asking to be removed from the sender’s mailing list.[40] Due to the additional effect that this has on the Internet Service Provider’s ability to continue to provide quality service to its customers, victims may also lose their account privileges for violating their ISP’s anti-spam policy.[41] The Spoofer effectively avoids liability for any of this wrongdoing, and his or her goal of sending unsolicited mass-mailings is achieved. This practice of cost-shifting - from deceptive spoofers to the Internet’s end user - has been likened to sending junk mail with postage due, or to making telemarketing calls to someone’s pay-by-the-minute cellular phone.[42] Both of which are concededly morally repugnant acts.

Internet Service Providers, who also become a victim to spoofing, assume the true costs of the mass distributions (aka “Spam”), as they are then forced to purchase additional servers to process the increased flow of e-mail messages. Failure to provide these additional resources will result in decreased quality of the service to customers. The reality of the situation is that the service could actually slow to a point of virtual stoppage.[43]

In addition to the tangible effects that this practice has on its victims, there exists the very real danger that the message that is forwarded under its illegitimate veil is actually a virus waiting to invade hundreds of thousand of computers.[44] What’s more, the unsuspecting recipient may even recognize the address. Thus, he or she will believe that the message was truly sent from a friend or family member, and then becomes the

first victim of the attack. He or she will open the e-mail, trusting its contents, and the virus will immediately then spread to each address that is listed within his or her address book, and pass on indefinitely. Thus, what is essentially a wasteful activity also poses a threat to the security and reliability of Internet communications.

The legal problem with spoofing:

The imposition of civil liability will be ineffective at serving as either a stiff deterrent or as adequate justice, notwithstanding its attempt to give back those costs that are imposed upon the ISPs, which are effectively evaded by the attackers. Without criminal liability, Internet Service Providers have neither the legal latitude nor the resources that government agencies have to investigate the frequent occurrences of spoofing. Nor would the Internet Service Providers have the authority that a governmental police task force or agency would have to invade the privacy of Internet users and thereby target the source of the attack. Under a criminal realm, a "cyberwarrant" of sorts could issue and provide greater hope for actually getting to the root of the problem, i.e. the Internet user who conceals his or her address when perpetrating an attack.

Additionally, the costs and the time investments that would have to be imposed upon the ISPs would be overly burdensome. The Internet Service Providers could not be expected to take on this burden alone. With civil liability, however, the right of action remains private. Accordingly, with presumably different levels of involvement and/or willingness to get involved among the ISPs altogether, it is possible that the quality of enforcement, if left to the ISPs, will not be consistent.

Considering the inability to find, and therefore enjoin spoof attacks, in combination with the continued imposition of attack costs onto the Internet Service Provider rather than the attacker, spoofing is unlikely to be deterred by mere threat of civil penalties alone. This is partly because the benefits to the attacker outweigh the nearly nonexistent costs, and in effect, serve as a disincentive for them to stop on their own. In its current state, spoofing is easy to do, difficult to trace, and worse yet, seemingly impossible to prevent.[45]

Current legislative attempts have their beginnings in 1997, when complaints were received from ISPs and their subscribers that an increasing portion of their time and resources was being wasted reading, sifting through, and deleting unwanted, unsolicited, and misrepresented mail.[46] While it appears as though legitimate[47] spam does have first amendment protection[48] as an arguably effective marketing tool, legislation that has been introduced or enacted aims at making sure that the mass mailing remains legitimate.[49]

Last year alone, thirty states introduced anti-spam legislation.[50] Of these thirty, seven states have already enacted their proposals. The twenty remaining states currently have anti-spam laws in place.[51] These laws, *inter alia*, strive to prohibit falsification and misrepresentation in the origin of, or the routing information on, the e-mail message.

It will seek to prohibit these offenses in two ways: by enjoining the behavior and by imposing a fine. That is to say, they will impose for the most part, civil liability. This civil legislation will most likely be ineffective at preventing spoofing. Without the ability to identify the attacker, money damages cannot serve to deter a spoofer from this practice, nor can an injunction effectively protect those who fall victim.

Pending Federal Legislation is flawed:

As of current, the act of spoofing is being viewed as a private action, rather than one against society. This classification thwarts legislation's aim of implementing the proper balance between punishing social harm and encouraging social good. The primary goal of criminal law is deterrence of those behaviors that cause social harm. Civil laws rely on the ability of one individual to combat societal offenses, one perpetrator at a time.

Current pending federal anti-spam legislation would seek to prohibit anonymous spam and forged headers, require opt-out or filtering procedures for consumers who wish to be deleted from spam lists or to not receive spam, and provide for civil liability for spamming violations.[52] Although this sounds promising, the inability of this legislation to succeed is illustrated by several examples.

Specifically, the "CAN SPAM Act of 2001" would require unsolicited commercial e-mail to have a valid return address to facilitate consumers' removal from spam lists, placing enforcement in the hands of the Federal Trade Commission. It would also permit Internet Service Providers to enforce violations of up to $10 per illegal spam.

The Coalition Against Unsolicited Commercial E-mail ("CAUCE") is pessimistic that this Act will be effective, being that this proposal is purely "opt-out." Spammers will still be able to send massive amounts of e-mail, shrouded in a veil of legitimacy, and recipients will have to be the ones who bear the burden of contacting each and every new advertiser.[53]

Some Federal Legislation, although on the right track, is also ultimately flawed.

The "Unsolicited Commercial Electronic Mail Act of 2001" was proposed in response to the plethora of new cyberpromoters that collect millions of e-mail addresses from service providers without their consent, mail to those who have already expressed desire to be kept off bulk e-mail lists, and/or purposefully disguise their identity or return address. The continued problem with these practices is in dealing with their refusal to yield to public pressure, private suit, or any other citizen action. If not stopped, the major concern is that such will overwhelm the Internet, and ultimately paralyze legitimate online commerce. The Act amends the Federal Criminal Code to provide criminal penalties for intentionally initiating the transmission of any unsolicited commercial electronic mail message to a protected computer in the United States, with knowledge that any domain name or other identifying information contained in or accompanying such message is false or inaccurate. The response to this form of Legislation is generally supportive, as it contains several acceptable provisions, i.e. prohibition on forgery

techniques, enforcement of ISP anti-spam policies, and provision of a private right of action for recipients and ISPs.[54]

While the proposal of this Bill seemed promising, the House Energy & Commerce committee's unfortunate decision was to pass a revised version, which effectively gutted the ISP policy provisions and replaced them with problematic provisions. According to CAUCE, the problem with these revisions is that the Act now requires a school, business, or ISP to first receive a flood of spam, before then being able to send a complaint. Only if a complaint is ignored would they then be able to sue under this law to stop further injury from resulting. Additionally, the Act requires a business or ISP to install expensive and complex filtering equipment as a requirement for enforcing it.[55]

A second proposal, the "Anti-Spamming Act of 2001" also seeks to amend the Federal Criminal Code. It would provide criminal penalties for intentionally initiating the transmission of bulk unsolicited electronic e-mail with knowledge that the message falsifies any of the following: Internet domain, header information, date or time stamp, originating e-mail address, or other identifier. It also makes illegal the sale or distribution of software whose purpose is to send messages with any of the above characteristics.[56] While this legislation is also on the right track, it is similarly unlikely to pass due to its over-inclusiveness. It prohibits technology that can have perfectly legitimate uses. The ultimate goal of anti-abuse legislation should, in fact, be to outlaw the acts of fraud, abuse, and trespass that are committed by crackers, not the tools they employ.

A final example, the "E-Mail User Protection Act," if passed, would seek to prohibit the sending of unsolicited bulk e-mail containing false sender information, a false return address, or other false header information. Spamming would be permitted, provided no forgery is involved.[57] Retribution under this Act would constitute a combination of civil and criminal liabilities. It would call upon the Federal Trade Commission ("FTC"), empowering it to enforce violations as unfair or deceptive trade practices.

It is again unlikely, however, that this legislation will be effective. CAUCE submits that this type of bill would actually be unacceptable to most service providers. In order to benefit from this Act, the inclusion of valid contract information in every UCE message would be required. Further, ISPs would be required to maintain and make available lists of their users who had requested to continue to receive UCE. Both domain owners and ISPs would be required to register their preferences with the Federal Trade Commission. While this is a burdensome requirement, it could also be quite confusing to match the domain names contained in e-mail addresses to the policies listed on an FTC master "opt-out" list. Additionally, CAUCE is adamant to opine that the terms of a contract between ISPs and its customers should not be dictated by D.C. legislators.[58]

Two additional Acts, the "Electronic Mailbox Protection Act of 1997" and the "Netizens Protection Act of 1997,"[59] also attempt to target distributions by unidentifiable senders, specifically to an electronic mail address of an individual with

whom such person lacks a pre-existing and ongoing business or personal relationship, unless said individual provides express invitation or permission. This lack of a pre-existing relationship is viewed as an increasingly serious threat to online commerce and personal privacy rights.[60] Similarly, however, the remedy sought is civil damages, which is arguably ineffective at deterring this offense.

Thus, it appears that legislation is taking a step in the right direction. For effectiveness and for consistency, however, federal legislation with teeth is crucial. The current proposals are not powerful enough. We must pull from our legislative history those statutes that have proved successful in traditional settings, and apply them to these modern parallels. Considering the inability of legislation to keep up with the speed of technological advancements, there is minimal opportunity to make incremental improvements. The first round of legislation has to be an immediate success.

Criminal liability is necessary

For the reasons that follow, the focus on stopping spoofing has shifted to the detriment of effective legislation. The focus should not be on spoofing as an aggravated form of spam because spam embodies first amendment protections to free speech. Rather, the focus should be on e-mailing and the Internet as an extension of writings and telecommunications, whereby forging an e-mail address in "cyberspace" constitutes forgery in the same way as is currently prohibited in "real space."

As a foundation for the analysis that follows, it is worth noting that it is not uncommon for a court to determine that the assumption of a false name and address constitutes a "consciousness of guilt"[61] on behalf of the perpetrator, where he or she has attempted to avoid detection for the crime that has been committed. Thus, when such an act of deception is carried out, criminal intent is presumed to have been present. The groundwork is then laid for imposing criminal liability, alone or in combination with civil liability, and the door to governmental investigation could effectively be opened to successfully trace the routing back to the perpetrator.

The investigative burden would no longer be on an ISP or end user, but rather on a governmental agency, having greater access, resources, and skills to identify wrongdoers and prosecute them. A criminal route needs to be taken, not only for efficiency and ease of prosecution, but also to better serve justice. Criminal sanctions punish social harm and encourage social good. These goals are unattainable through continued reliance on civil actions. First, private individuals have limited resources with which to identify spoofers. Second, mass e-mailers are not deterred by insubstantial civil judgments, as such judgments are often greatly outweighed by the fruits of spoofing activities.

It is undisputable that a United States citizen may not have his or her privacy invaded without probable cause that there has been some unlawful act committed.[62] Only then is the government justified in stepping in to remedy that wrong. Spoofing is a

cyber wrong, and the perpetrator of the attack must not be allowed to mask his or her identity and maintain an undeserved privacy.

It is, on the other hand, arguable that an Internet user does not at all have a reasonable expectation of privacy, however it is still very much an open question.[63] The U.S. Supreme Court has stated that American citizens have the protection of the Fourth Amendment guarantee of freedom from search and seizure absent a warrant, when there is a reasonable expectation of privacy.[64] Without a reasonable expectation of privacy, however, there is no privacy right to protect. If the Internet user relinquishes his or her desire to maintain privacy by communicating through networks over what are essentially public lines, be they telephone wires or cables, he or she in essence may waive the right to maintain that privacy, and criminal search and seizure principles would not even be necessary.

The United States Supreme Court's decision in *United States v. Katz*[65] sets forth the foundation for both federal and state constitutional law analysis with respect to constitutionally protected privacy expectations. Thus, any discussion of whether an internet user has a justifiable expectation of privacy that is protected from unreasonable searches and seizures must necessarily begin with *Katz*.[66] In his concurring opinion, Justice Harlan articulated his view of the appropriate inquiry with respect to determining privacy rights under the Fourth Amendment. In determining in which areas a person has a constitutionally-protected expectation of privacy, Justice Harlan set forth a two-fold requirement that a person: (1) have exhibited an actual (subjective) expectation of privacy; and (2) that the expectation be one that society is prepared to recognize as reasonable.[67]

This two-pronged test has been the basis for the finding that a reasonable expectation of privacy does not exist.[68] In *Rekasie,* the Pennsylvania Supreme Court wrote that while the defendant might have possessed an actual or subjective expectation of privacy in his telephone conversation, because of the nature of telephonic communication, it is not an expectation that society would recognize as objectively reasonable. The Court explained, “[a] telephone call received by or placed to another is readily subject to numerous means of intrusion at the other end of the call, all without the knowledge of the individual on the call.”[69] Thus, following a similar analysis in the Internet realm, it is likely that a court may also find that it is not objectively reasonable for one to assume an expectation of privacy when mass distributing thousands of e-mails. Coupled with a presumption of criminal intent due to the aforementioned consciousness of guilt discussion, the argument for the imposition of criminal liability is bolstered.

Assuming arguendo that a reasonable expectation of privacy does exist over the lines of Internet communication, the principles of search and seizure would then be necessary within the institution of criminal liability. A “cyberwarrant” of sorts would be issued based on having the requisite probable cause, and it would enable the proper governmental agents to effectively get to the source of the offense, i.e. the initiator of the spoofed e-mail. This aspect of righting the wrong would essentially be impossible by means of a civil route to justice. The combination of civil penalties with criminal will be

the most effective strategy, as it would give those costs incurred back to the injured ISPs, will effectively punish the wrongdoer, and will deter a large portion of future attacks by illustrating that the wrong will be immediately discovered, investigated, and prosecuted.

Progressive state legislative history treats criminal liability as effective:

In analyzing traditional state legislation, one can see that the offenses sought to be prohibited in real space are analogous to those that we now seek to prohibit in cyberspace. Two common law offenses that this author proposes to be similar in regards to effectively prosecuting spoof attacks are those of forgery and mail fraud, each of which are subsequently discussed.

In 1992, New York was one of the first states in the nation to address the problem of telecommunications fraud and theft, by enacting legislation that resulted in prosecution and conviction of these offenders.[70] Subsequently, other states followed suit. Currently, however, the majority of state legislatures that are attempting to target spoofing are proposing that the penalties imposed be civil. New York parts from this majority and seeks to impose criminal liability for these offenses. New York should again be allowed to pave the way for prosecution and conviction of offenders that use the Internet to commit forgery and fraud.

NY CLS Penal § 170.00 (2002) defines a forged instrument as a "written instrument which has been falsely made . . . or altered." Further, a "written instrument" includes "computer data or a computer program . . . containing written or printed matter or the equivalent thereof . . . which is capable of being used to the advantage or disadvantage of some person." Something is "falsely altered" when, "without the authority of anyone entitled to grant it, [the forger] changes a written instrument . . . so that such instrument in its thus altered form appears or purports to be in all respects an authentic creation of or fully authorized by its ostensible maker …."[71]

Although, traditionally, a "written instrument" has been thought of in the pen and paper sense, applying this code to a technological setting would not be such a foreign notion. Although few would conceive of technology as constituting a "written instrument" for purposes of applying the code, the definitions of "forged instrument" and "written instrument" are sufficiently broad to include such technology.[72] In fact, even under common law notions, the Supreme Court of the United States was not satisfied that forgery was limited to the production of a writing by means of only a pen.[73] The Court concluded that the nature of the crime of forgery was not changed whether it was committed by "printing, or by stamping, or with an engraved plate, or by writing with a pen."[74]

In State of *New York v. Miguel Pena*,[75] the court held that the evidence sufficiently established that a cellular phone was a "written instrument" and that a "cloned telephone" was a forged instrument because it fit the definition of a written instrument and had been falsely altered. The court further determined that the evidence sufficiently proved that the defendant had possessed, with knowledge of its character,

equipment specifically designed for use in counterfeiting or otherwise forging numbers for the purpose of cloning cellular telephones. Thus, the defendant was convicted on criminal possession of a forged instrument in the second degree, criminal possession of computer related material, and criminal possession of forgery devices.[76]

Following such a rationale, it can further be determined that the spoofer also possesses, with knowledge of its character, equipment that is specifically designed for use in alteration. That is, "sniffing software" could be considered to be an illegitimate device in the forgery scheme,[77] and possession of that device presents consciousness of the perpetrator's guilt. This is so when no other purpose for having such a device is provided.

The essence of any forgery crime is the intent to defraud or injure.[78] So being, this author proposes that an e-mail must also fit into the definition of a written instrument, wherein changing the routing information or the content of the message would then constitute fraudulent and material alteration thereof.

"To 'falsely alter' [computer data] means to change [computer data] without the authority of anyone entitled to grant such authority, whether it be in complete or incomplete form, by means of erasure, obliteration, deletion, insertion of new [data], transposition of [data], or any other means, so that such instrument in its thus altered form falsely appears or purports to be in all respects an authentic creation of or fully authorized by its ostensible maker."[79]

II. Fraud

States began enacting legislation in the 1930's, which sought to deter and to punish use of the mails to defraud or misrepresent the public. To succeed on a claim that is based on acts of mail and wire fraud, a plaintiff must prove (1) the existence of a scheme to defraud, (2) the participation by the defendant in the scheme with the specific intent to defraud, (3) and use of the Postal Service or interstate telephone to defraud must involve some sort of fraudulent misrepresentations or omissions reasonably calculated to deceive persons of ordinary prudence and comprehension.[80] Plaintiffs must prove that defendant either devised the fraudulent scheme itself, or willfully participated in it with knowledge of its fraudulent nature.[81] This requisite intent to defraud may be proven by either direct evidence or demonstrated circumstantially.

It is seemingly clear then, that the use of public phone lines to send electronic mail might also constitute mail fraud and fit within the definition thereof.

As previously demonstrated, spoofers generally alter the origin of their spam and e-mail messages for the purpose of avoiding the hostile reaction that they intend and often do receive from their bulk mailings. This illustrates the existence of a scheme to defraud the recipient. Additionally, with involvement of the proper governmental agencies, the second prong of the mail fraud requirements may also be met - the participation of the defendant in this scheme to defraud. With the mere imposition of civil

liability, the responsibility would be solely on the individual recipient of the spoof to determine the sender's identity alone - clearly an impossible task.

Current state legislatures have attempted to modernize the prohibition of fraud in communications. One of the first judicial tests took place in the state of Washington last year. In *State of Washington v. Heckel*, respondent began sending unsolicited commercial e-mail (spam) over the Internet.[82] His intention was to market a book that he had written, but his hundreds of thousands of weekly e-mails contained false and misleading information in the subject line.[83] The state Supreme Court declared that Washington's commercial electronic mail act was sufficiently limited to reach deceptive e-mails and that the local benefits of the Act outweighed any burdens placed on those sending commercial e-mail messages.[84] While the Superior Court's concern when it declared the anti-spam law unconstitutional was whether a state should be involved in the regulation of the Internet, the Supreme Court's subsequent reversal and remand for trial indicates that when the perpetrator is identifiable, the courts will take an active role in stopping this unlawful behavior, provided that the Act enables them to impose adequate liability.

Stressing the importance of criminal liability from this angle as well, criminal investigation would enable the routing of the spoofed e-mail to be traced back to the perpetrator's account, by tracking the nodes through which it passed en route to its destination. The requirement of the ISP then, would be to disclose the name of the user who owns the address. The ISP will additionally be benefited as it will presumably then be able to prosecute the violation of its anti-spamming policy. Additionally, it may well be that this information is public - headers are readily viewable with some of the more popular mail clients - assuming this part is not that which has been altered, the attacker is readily identifiable.[85]

Where the originator is not readily identifiable, however, an investigation would ensue to trace the origin of the e-mail. The investigation could entail, for one, detection of whether or not sniffing has occurred to wrongfully pull messages off the network. Furthermore, since each packet passes through various nodes in the destination chain, there will be an electronic record kept of that path which can be reversed back to the point of origination. With the determination that a crime has been committed, Title 18 of the U.S. Code could then apply in order to access stored electronic communication and records. Under this Title, "a governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire of electronic communication, that is in electronic storage in an electronic communications system . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation."[86]

Current State Legislation

As previously mentioned, thirty states have introduced anti-spam legislation in the last year, seven of which have already enacted their proposals. The twenty remaining states currently have anti-spam laws in place. A closer look at the twenty-seven enacted

statutes, however, reveals only two states with impositions of criminal liability, or a mix of civil and criminal liabilities.[87] Although this is a small percentage, the fact that these states have proposed criminal liability for this cyber wrong at all supports this author's argument.

The best approach would be the federal enactment of a uniform prohibition against spoofing altogether, criminally sanctionable in cases of violation. Although state legislation is encouraging, federal legislation is preferred, since transmitters of unsolicited bulk e-mail can easily move from state to state to carry out their feat.

Judicial intervention can take prohibition of cybercrimes only so far

The courts have generally been successful in stopping aggravated spam, as distinguished from spoofing. With aggravated spam, a more moderate form of spoofing, an unsolicited commercial e-mailer can be enjoined under such theories of trespass to chattel and computer fraud.[88] The main distinction here is that the spammer creates an e-mail account and will falsify point-of-origin information, i.e. use a victim's domain name (generally the Internet Service Provider[89]) for the purpose of transmitting mass amounts of e-mail. When liability attaches, it is for misappropriation and dilution of trademark. In these cases, the ISP has a better chance of identifying the perpetrator. In the case of spoofing, however, the origin of the e-mail is completely disguised. This means that an e-mail distribution can be delivered appearing to have initiated from the address of either you or me. Any investigation by the ISP under this scenario would ultimately reach a dead end with the arrival at the complainant or the victim. Moreover, if enjoined by the courts, there is nothing to prevent the spoofer from simply creating a new website and continuing this operation without pause.

Prevention by criminal deterrence and technology

Legal Approaches:

In addition to the attempts to provide legislative relief for this growing concern, the government has also implemented the "Computer-Telecommunications Coordinator" (CTC) program.[90] Under this program, each United States Attorney's Office, as well as a few other Department entities, has designated at least one Assistant U.S. Attorney to handle certain responsibilities.[91] This provides encouragement that the Internet will be more satisfactorily monitored and regulated.

Technological Approaches:

While the easiest approach for individual end users annoyed by spam is just to ignore the unwanted messages, there are technological ways to put an end to, or at least lessen, the severity of the attacks. In response to the ever prevalent question of what types of approaches should be taken to prevent spoof attacks, the answer is part legal and part technical.

For the more innocent types of bulk e-mailing, a good place to begin is with your own computer, in an attempt to trace the bulk e-mail back to its generator. Within most operating systems, there is software entitled “TraceRoute.”[92] Given the domain name or an IP address, this software will diagram the net from your server to the server you have specified, showing you all the nodes along the way through which the message was routed.[93] The last node will be the domain or IP address of the source of the message that was received, and the next to last node will be the domain of the upstream provider of the owner of the domain you specified.[94] While this might not get you a valid e-mail address for contacting the generator directly, it will put you in touch with their upstream provider, the companies that sell them Internet access.

Companies who legitimately send bulk e-mail for marketing purposes under their first amendment protection should be encouraged, if not required, to utilize data mining and targeted e-mail approaches to ensure that the mail they send is delivered only to interested parties. In addition, requiring opt-in plans would avoid wasting consumers’ time, as well as alleviate some of the taxing on Internet Service Providers who must handle the mass of e-mail distributions.

Since spoofers have learned how to take advantage of known holes in the operating system with a static IP address, the solution to spoofing starts with a firewall that redirects any unknown requests and provides a barrier to mask the IP addresses of workstations on the network.[95] Individual consumers as well as companies can have firewalls installed, which serve as gatekeepers, and control which e-mail addresses can enter and which can exit. They do not, however, control one’s actions once they are permitted to enter. Firewalls are designed to slow attackers down, not to stop them completely.[96]

Secondly, a company can filter their e-mail traffic in order to prevent IP spoofing. With ingress filtering, IP traffic with one’s internal IP range should not be permitted to enter that network from an external source. Conversely, with egress filtering, one is prevented from within the network, from sending out IP traffic with an origination address that is outside your IP range.[97] One thing to be aware of, however, is that while most filtering techniques involve rejecting messages that appear to be spam, it is also possible to reject all inbound messages except those that can be recognized as legitimate, which could be as limiting as allowing mail from only those addresses which are in the user’s address book.

A third possibility would be to protect yourself from spam by distributing your e-mail address in a form that is invalid for a program that specifically searches for e-mail addresses, but that is readable for a human.[98]

Lastly, one of the most powerful and effective modes of protection, is encryption. Encryption software scrambles the data with a secret code so that no one can make sense of it while it is being transmitted.[99] When the data reaches its destination, that same software unscrambles the information so that it can be understood by the recipient.[100] Encryption can virtually guarantee that “sniffers” will not be able to read the data

contained within the packets that they detect.[101] The text is essentially unintelligible. Moreover, encryption can provide certainty that any message received was transmitted by the individual purporting to have sent it.[102] Certain encryption software can even scramble the packet header information so that it is impractical to spoof the message at all.[103] After all, "Unlike paper mail, the world of electronic mail is a world of postcards. The prudent user will place his messages in the 'envelope' of encryption."[104]

Although there are precautions that the Internet user may take to mitigate the effects of and prevent against a spoof attack, the real solution lies in focused legislation with enough clout to make an impact on a daily basis. This threat to modern communication should not be underestimated, as the security of the Internet, as well as the flourishment of e-commerce could be at stake. Until that happens, technological deterrence will somehow have to suffice.

---

* Juris Doctor candidate, May 2004, University of Pittsburgh School of Law.

[FN1] David Lerner, *Seeking to Clear Cyberspace of Spam: Recent Court Decisions Boost Efforts to Regulate Unsolicited Commercial E-Mail*, 227 N.Y.L.J., June 10, 2002, at 4 col.

[FN2] *See* Mario Morino, Point of View: Technology as a Social Benefit Tool, at http://www.childrenspartnership.org/pub/next/0398/social.html. (last visited July 27, 2003).

[FN3] John S. Quarterman & Peter H. Salus, *How the Internet Works*, http://www.mids.org/works.html, (last modified December 18, 1999).

[FN4] *Id.*

[FN5] *Tracking Spam, at* http://www.claws-and-paws.com/spam-1/tracking.html. (last visited July 27, 2003).

[FN6] Robert L. Jones, *Client Confidentiality: A Lawyer's Duties with Regard to Internet E-Mail*, (August 16, 1995), *at* http://www.kuesterlaw.com /netethics/bjones.htm.

[FN7] The Domain Name Suffix is known as the Top-Level Domain Name, and describes the type of organization. The most common TLDs and what they signify are: .com - commercial, .edu - educational, .org - non-profit organization, .mil - military, .net - network provider, .gov - government agency, .biz - businesses, .info - all uses, and .museum - museums. There are also 244 national TLDs which were established for their respective countries. *Learn the Net.com, Surf the Web: Domain Names, at* http://www.learnthenet.com/english/html/84domain.htm, (last modified April 9, 2003).

[FN8] Quarterman & Salus, *supra* note 3.

[FN9] *Id.*

[FN10] *Id.*

[FN11] *Id.*

[FN12] *See* A Hacker's Tools of the Trade, PBS Frontline, February 2001, *available at* http:/www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/tools.html.

[FN13]Netlingo, *Trying to Figure it all out: NetLingo Makes Sense, at* http://www.netlingo.com/inframes.cfm (last visited July 27, 2003).

[FN14] *Id.*

[FN15] Netlingo, *supra* note 13.

[FN16] Quarterman & Salus, *supra* note 3.

[FN17] *Id.*

[FN18] *State v. Heckel*, 24 P.3d 404, n.4 (Wash. 2001).

[FN19] *See* Quarterman & Salus, *supra* note 3.

[FN20] Heckel, 24 P.3d at 404. n.4

[FN21] Jones, supra note 6.

[FN22] A spoof, first and foremost, may take several forms. While this Note will deal mainly with the type concerning forged e-mail addresses, it is worth mentioning that a website and a domain name can also both be spoofed.

When a website is spoofed, the objective may be content theft, where a copy of the site is created from the original and placed onto another server. Or, a parallel website may be created, that a user reaches by inadvertently mistyping the name of the attempted website. Thirdly, a cracker may alter a link within a webpage by inserting his address before the actual address, so when a user clicks on the link, the cracker's site is visited, rather than the real site.

Alternatively, a domain name can be spoofed when the attacker alters an entry on a server's massive database, so that the spoofer's domain name matches up with the numerical IP Address of an innocent company. This may be done to steal business from another company via redirecting the consumer to their website unknowingly. *See* ArticSoft, Spoofing - Arts of Attack and Defense, *at* http://www.articsoft.com/whitepapers/spoofing.pdf (last visited July 27, 2003).

[FN23] A “cracker” is someone whose interest includes unauthorized entry and modification of computer systems. Although not the case, this term has become synonymous with the term “hacker,” who is someone intensely interested in complex computer systems, but is often a systems operator or administrator who detects, repairs, and prevents the break-in and damage done by “crackers.” Jones, *supra* note 6.

[FN24] Articsoft, *supra* note 22.

[FN25] Rik Farrow, *Source Address Spoofing: Forged Addressess aid Internet Attacks. Here’s What to do About Them,* NetworkMagazine.com, May 1, 2000, *at* http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleID=8702815.

[FN26] *Carnegie Mellon Software Engineering Institute Coordination Center, Spoofed/Forged Email, at* http://www.cert.org/tech_tips/email_spoofing.html (last modified September 4, 2002).

[FN27] *Id.*

[FN28] As opposed to the Application layer lever, where attacks such as viruses frequently occur. *See* K-12 Linux, K12Linux Network Administration Course: Task 6: Firewalls & Security, *at* http://www.k12linux.org/netadmin/security.php3, (last visited July 27, 2003).

[FN29] A similar, though less egregious method of gaining access into a secured site involves IP Address changing attacks. Crackers are able to configure themselves to have any IP Address that they choose, and in doing so they can appear to be part of an internal network, when if fact they are external. Articsoft, *supra* note 22. It is in this way that the cracker can carry out their sordid acts.

[FN30] *Harry A. Valetk, Spam Scammers hit a new low with Spoofed E-Mail,* 228 N.Y.L.J., September 16, 2002, at 6 col. 1.

[FN31] Sniffing is actually a legitimate and necessary function of a network’s administrator, who monitors network traffic to ensure proper functionality. Jones, *supra* note 6.

[FN32] *See Id.*

[FN33] *Id.*

[FN34] *Id.*

[FN35] *Id.*

[FN36] *Supra*, note 6.

[FN37] Valetk, *supra* note 30.

[FN38] *Id.*

[FN39] Lerner, *supra* note 1.

[FN40] Valetk, *supra* note 30.

[FN41] *Id.*

[FN42] *State v. Heckel*, 24 P.3d 404, 410 (Wash. 2001).

[FN43] At times, this mass e-mailing can be targeted to a specific e-mail address, causing that e-mail account to crash and the user is rendered unable to access their account. This is commonly referred to as "bombing" in Internet terms. E-mail bombing is characterized by abusers repeatedly sending an e-mail message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact. *See* CERT Coordination Center, E-mail Bombing and Spamming, *available at* http://www.cert.org/tech_tips/e-mail_bombing_spamming.html. (2002).

[FN44] *See* Richard Raysman and Peter Brown, *Computer Security Breaches - Who May Be Held Responsible?* 227 N.Y. L.J. May 14, 2002, at 3.

[FN45] Valetk, *supra* note 28.

[FN46] Lerner, *supra* note 1.

[FN47] Legitimate spam can be classified as such if it does not commit one of the many potential offenses to which spammers are susceptible: false designation of origin, dilution of interest in service marks under the Lanham Act, state and common law unfair competition, exceeding authorized access and impairing computer facilities in violation of the Computer Fraud and Abuse Act, violation of state computer crimes acts, deceptive trade practices, defamation, forgery, harassment, theft, libel, breach of contract, false statements in advertising, and/or common law trespass to chattels.

Dianne Plunkett Latham, *Electronic Commerce in the 21st Century: Article Spam Remedies*, 27 WM. MITCHELL L. REV. 1649, 1651 (2001).

[FN48] Jan H. Samoriski, *Jan H. Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?* 43 THE JOURNAL OF BROADCASTING AND ELECTRONIC MEDIA, (2000).

[FN49] *See* National Conference of State Legislatures, State Laws Relating to Unsolicited Commercial or Bulk E-Mail (SPAM), *at* http://www.ncsl.org/programs/lis/legislation/spamleg02.htm. (last modified June 1, 2003).

[FN50] *Id.*

[FN51] *Id.*

[FN52] *See* Netizens Protection Act of 1997, H.R. 1748, 105th Cong. (1997); Unsolicited Commercial Electronic mail Choice Act of 1997, S. 771, 105th Cong. (1997); Electronic Mailbox Protection Act of 1997, S. 875, 105th Cong. (1997).

[FN53] CAUCE: Coalition Against Unsolicited Commercial E-mail, *available at* http://www.cauce.org/legislation/index.shtml (last modified May 12, 2003).

[FN54] *Id.*

[FN55] *Id.*

[FN56] *Id.*

[FN57] *Id.*

[FN58] *Id.*

[FN59] This Act would amend the Communications Act of 1934 to ban the transmission of unsolicited advertisements by electronic mail. H.R. 1748, 105th cong. (1997).

[FN60] *See* Electronic Protection Act of 1997, S. 875, 105th Cong. (1997); and Netizens Protection Act of 1997, H.R. 1748, 105th Cong. (1997).

[FN61] *See generally*, State v. Riser, 800 A.2d 564 (2002).

[FN62] The Fourth Amendment limits government's power to invade privacy. It reads as follows: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." *See* U.S. CONST. Amend. IV.

[FN63] At least in the workplace setting, courts which have considered this issue have generally held that employees do not have a reasonable expectation of privacy in e-mail messages sent via a system provided by the employer. *See* Daniel L. Appelman, The Law and the Internet: Emerging Legal Issues, INTERNET SOURCE, May 11, 1995 *available at* http://www.isoc.orp/HMP/PAPER/222/txt/paper.txt.

[FN64] *See generally* United States v. Katz, 389 U.S. 347 (1967).

[FN65] *Id.*

[FN66] In *Katz*, governmental agents attached an electronic listening and recording device to the outside of a public telephone booth and were able to overhear the defendant discussing wagering information over the telephone. The Court determined that the government's electronic listening to, and recording of, the defendant's words violated the privacy upon which he justifiably relied while using the telephone booth. *See Id.*

[FN67] *United States v. Katz,* 389 U.S. 342, 360-61 (1967) (Harlan, J., concurring).

[FN68] *Commonwealth v. Rekasie,* 566 Pa. 85, 93 (2001).

[FN69] *Id.* at 95.

[FN70] Rasch, Mark D. Legal Lessons in the Computer Age, *available at* http://www.securitymanagement.com/library/000122.html See NY CLS Penal § 170.00 (McKinney 2002).

[FN71] *See* NY CLS Penal § 170.00 (McKinney 2002).

[FN72] *Benson v. McMahon,* 127 U.S. 457, 467 (1888).

[FN73] *Id.*

[FN74] *Id.*

[FN75] 642 N.Y.S. 2d 807

[FN76] *Id.*

[FN77] A packet sniffer is a wiretap device that plugs into computer networks and “eavesdrops” on network traffic. Since network traffic consists of binary data, sniffers come with "protocol analysis" which decodes the binary traffic. Most sniffers are capable of decoding common TCP packets. *See* Michael Sink, The Use of Honeypots and Packet Sniffers for Intrusion Detection, SANS INSTITUTE, Apr. 15, 2001 *available at* http://www.sans.org/rr/intrusion/honey_pack.php.

[FN78] *Powers v. State*, 333 So. 2d 205, 207 (Ala. Crim. App. 1976).

[FN79] Colo. Rev. Stat. 18-5-101 (2002).

[FN80] 18 U.S.C.S. § 1342 (2002).

[FN81] *Id.*

[FN82] 24 P.3d 404 (2001).

[FN83] *Id.*

[FN84] *Id.*

[FN85] For an explanation of how you can defeat the attempts of spam generators to mask their identities, *see* TraceRoute, *available at* http://mindworkshop.com/alchemy/nospam.html.

[FN86] 18 U.S.C.S. § 2703(a) (2002).

[FN87] NCSL.org, *supra*, note 49.

[FN88] *See generally* Compuserve, Inc. v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997); *America Online v. IMS*, 24 F.Supp. 2d. 548 (E.D. Va. 1998).

[FN89] In *America Online, Inc. v. LCGM*, AOL sued when defendants forged the domain information "aol.com" in the "from" line of the e-mail messages sent to AOL members and caused the AOL domain name to appear in the electronic header information of the commercial e-mails. The court granted AOL's motion for summary judgment. *See* America Online, Inc. v. LCGM, 46 F. Supp. 2d 444 (E.D. Va. 1998).

[FN90] *CriminalDefense.com, How Does the Government Regulate the Internet?* (July 29, 2002), *at* http://www.criminaldefense.com/computer_government_regulation.html.

[FN91] *Id.*

[FN92] Mindworkshop.com, *supra* note 85.

[FN93] *Id.*

[FN94] *Id.*

[FN95] Securing the E-Mail, *available at* http://www.geocities.com/Colosseum/Ring/5052/E-Mail7.html. (Last visited August 1, 2003).

[FN96] CERT Coordination Center, *supra*, note 26.

[FN97] *Id.*

[FN98] Andreas Krennmair, *Why forging E-mail Addresses Is A Bad Thing, (November 2, 2001), available at* http://www.synflood.at/tack/texts/forge-e-mail.pdf. (Last visited August 1, 2003).

[FN99] Learnthenet.com, *available at* http://www.learnthenet.com/english/html/84domain.htm (last updated January 23, 2001).

[FN100] *Id.*

[FN101] Jones, *supra* note 6.

[FN102] *Id.*

[FN103] *Id.*

[FN104] *Id.*