;login:

THE MAGAZINE OF USENIX & SAGE

April 2004 • volume 29 • number 2

inside:

THE LAW

Egelman: Suing Spammers for Fun and Profit

USENIX

The Advanced Computing Systems Association

suing spammers for fun and profit

by Serge Egelman

Serge Egelman is an undergraduate in Computer Engineering at the University of Virginia. He expects to graduate next month barring any unforseen difficulties. He plans to continue battling spammers on the side as a graduate student next year

serge@guanotronic.com

How would you like to expand a body part by up to 30%? What would you say if you could get your degree from a leading non-accredited university for just three easy payments of . . . . Okay, we all see it every day, spam advertising everything from low-interest mortgages to an Extreme Colon Cleanser. A few recent studies have shown that spam, or unsolicited commercial email, accounts for nearly 50% of all email this year. That number is rapidly increasing.

Personally, I receive about 80 messages a day, though I have friends who receive 500–1000 messages. I run my own mail server with a fairly common Sendmail configuration; I subscribe to the black-hole lists and have all the default spam prevention measures enabled. I also use SpamAssassin (*http://www.spamassassin.org*) to sort most of my spam (procmail puts all the tagged spam into a different mailbox). However, almost a dozen messages still get through to my main mail spool each day. It is rather annoying, and so I have started taking action.

Last year I happened to notice that my state, Virginia, has an anti-spam law. Since then I have been archiving all my spam, tracking down those responsible, and taking them to court. The following is a summary of what I have done, what I have learned, and what you can legally do to decrease your spam volume.

DISCLAIMER: The following is just a personal account of my experiences and should in no way be interpreted as legal advice. I am not a lawyer and do not claim to be one. Additionally, all quotes contained herein are from memory and are therefore not verbatim.

The Laws

In 1997, Nevada became the first state to pass legislation regulating spam, and currently 35 states have passed spam laws. The state laws share many similarities. They make it illegal to send messages with forged headers, deceptive subjects, no opt-out mechanism, or no clear indication in the subject line that the message is indeed an advertisement. States that have laws use some subset of these requirements (e.g., Virginia makes it illegal to falsify header information, whereas New Mexico only makes it illegal to omit "ADV" from the subject line). The legislation also outlines civil remedies, and a few states go so far as to make sending unsolicited email a criminal offense.

What this means is that if you are in one of the 29 states that provide for a civil action, you can start taking spammers to court and getting awarded statutory damages for all the spam that you receive. The majority of these laws provide $10 per message, but a few (California and West Virginia) go as far as allowing $1000 per message, as well as all associated legal fees. Some of the states that do not allow civil actions on behalf of the recipient or the ISP allow complaints to be filed by the state attorney general (in the case of Pennsylvania, the attorney general shall remit 10% of the damages collected to the person who filed the complaint).

The main problem with current legislation is that it is not unified; though similar to each other, laws vary from state to state. Some state laws grant personal jurisdiction to the court over out-of-state spammers, some require the spammer and the recipient to be in the same state, and some require the spammer to have knowledge that the recipient is in a particular state. What is needed is a federal law to regulate all spam sent within this country.

In fact, the 108th Congress saw nine such bills, one of which, the 2003 CAN-SPAM Act, was signed into law at the end of last year and went into effect on January 1. The law outlines many of the aforementioned requirements for sending unsolicited mail.

First, it is illegal to send a message with forged header information. The law defines header information as:

> "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message."

Essentially, it is illegal to put any false information in any part of the header. Next, the law makes it illegal to use deceptive subject lines. This is clarified by saying that the subject must not mislead a recipient "acting reasonably under the circumstances."

Finally, the law regulates the opt-out mechanisms that each message must contain and what must happen after a recipient has notified the spammer. Each message sent must contain either a URL or an email address to which the recipient can respond in order to opt out. Furthermore, this address must be functioning for at least 30 days after the original message was sent. The sender is also required to include his or her physical postal address. Upon being notified by the recipient, the sender has up to 10 days to cease sending further spam. Finally, the law mandates that the FTC outline a plan for implementing a nationwide Do-Not-Email registry within the next six months. This, of course, is similar to the Do-Not-Call registry. While this law has many provisions for regulating commercial email, the main question is, how are they to be enforced?

The CAN-SPAM Act provides a few different measures for enforcing the new restrictions. The law provides both criminal and civil penalties. A defendant deemed guilty can be fined and/or imprisoned for up to three years for the first offense. Repeated offenses can carry prison terms of up to five years. In terms of enforcement, the FTC is granted the most power; however, state attorneys general can also bring cases to court. Since this is a federal law, cases can be brought in any US district court. In terms of statutory damages, the FTC or a state attorney general can seek up to $250 for each message sent in violation of the law (up to a maximum of $2 million for any offense other than falsifying header information).

Unfortunately, the law is sparse on private civil remedies. The only private right of action that is outlined is for ISPs. ISPs that receive spam may take the spammer to court and claim statutory damages of $100 for every forged message and $25 for every message that violates any other part of the statute. Additionally, legal fees can be claimed. This, though, is a two-way street: The defendant may also claim legal fees if they get a favorable ruling. While this is the only private civil action that may be pursued, it might be available to more people than one might think. The law defines an ISP as any entity that provides email or any other Internet service to others. Thus, anyone who provides email or shell accounts is technically an ISP and can therefore pursue spammers under this law. However, in addition to the risk of losing and having to pay the spammer's legal fees, there is another downside: this law can only be used in a federal court, so in addition to the increased filing fees, you will most certainly need a lawyer.

While it is clear that this law has potential, there is much criticism surrounding it. Last year, the Direct Marketing Association (DMA) spent millions of dollars lobbying against the newly implemented Do-Not-Call registry. This legislation was a huge blow to the telemarketing industry (many telemarketing companies belong to the DMA). It might come as a surprise to hear that the DMA has been heavily lobbying in favor of the CAN-SPAM Act (affectionately called the I-CAN-SPAM Act by many anti-spam-

mers). Just recently, California amended their existing anti-spam laws to make the sending of any spam illegal (instead of just imposing restrictions, like most other states). This new law was set to go into effect on January 1. Unfortunately for Californians, the *federal* law contains a preemption clause:

> This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

This means that any state law that outright bans spam is now null and void. However, laws that only regulate deceptive spam (e.g., outlawing forged headers or fraudulent subject lines) will remain. While the new CAN-SPAM law outlines certain restrictions on how messages can be sent, it takes an opt-out approach: It is perfectly legal to send spam to recipients until they say to stop (or, more accurately, 10 days after that time). This, of course, leaves open the possibility for a spammer to sell the email address to someone else (and thus the recipient has to tell all subsequent spammers to stop). Additionally, the law legalizes spam sent from someone with whom you have an existing business relationship.

This is why it's no surprise that the nation's largest ISPs have heavily backed this legislation. Most media outlets have two sources of revenue: the subscribers who pay for the service, and the advertisers who pay to get their message seen by the subscribers (e.g., you pay for cable television, yet still have to endure commercials). This business model is now moving to ISPs. You pay them for an email account and Internet access; now they can legally send advertisements for additional revenue. Furthermore, it protects this business model in that they can forward you spam from companies who are paying and in turn pursue those who spam and have not paid for the privilege.

With all the more serious crimes occupying the time of the FTC and others charged with enforcing this act, it's laughable to believe that they will be devoting large efforts to enforcing it. In fact, California has had an anti-spam statute for a few years, yet the first criminal conviction occurred only a few months ago. The DMA and others who lobbied for the CAN-SPAM Act also understand this. In fact, when the bill was signed into law, Bill Gates wrote an article hailing this as a tremendous victory. Clearly, in the coming months we can expect a whole line of ludicrously priced Microsoft anti-spam products. So while this law probably won't reduce the flow of spam by itself, individuals . . . errr . . . "small ISPs" can still take action by saving spam and tracking down those responsible.

Tracking Down the Spammer

Spammers' use of open relays and forged addresses discourages most people from bothering to hunt down the sources of their spam. While there is still a lot of spam that comes from legitimate return addresses, most spammers go out of their way to obfuscate the origin. The fact of the matter remains, however, that they are trying to do business with you and therefore need to leave a way for you to contact them. Naturally, this means that they will include a URL for their Web site.

There are many tools online that can aid in locating the origin of your spam. The site that I use the most is Spamhaus (*http://www.spamhaus.org*). They have a running database of known spammers and known IP blocks that host spammers. Most spammers

will use fake whois information, so this site is an invaluable tool. Simply enter the IP address corresponding to the URL and, hopefully, it will return the lucky winner. If there are no hits, there is a good chance that the IP address of the corresponding DNS server (taken from the whois information for the advertised domain name) might be in the Spamhaus database. Spammers purchase large IP blocks and will often use them for spamming once or twice before moving on to a different IP block, but changing the IP of a DNS server so frequently is a lot more difficult.

If you have gotten lucky and have found a name and address for a spammer, the next step is to locate the address for their "registered agent." This is their retained attorney, whom you will serve with the court summons. This information is available online in most states and, by law, is required to be on file with the Office of the Secretary of State (or equivalent) in the state where the company is incorporated. Finding the address of the registered agent is often as simple as going to the secretary of state's Web site and using an online query tool. Some states charge for this information, but it is still publicly available. If all else fails, you are probably safe just using the regular business address of the company.

So You Are Going to Court

The first time I did this was in March of last year; I had received 80 messages sent by Etracks.com, Inc., a California-based marketing company. After the first message I received from them, I sent a response explaining that they had violated state law, and if they continued to do so I would not hesitate to settle this matter in court. Naturally, I never received a response, and the spam continued. So I went to the local courthouse to file a complaint in small claims court.

A friend who had been to small claims court a few times gave me some invaluable advice: Know exactly what you want before you go to the clerk's office, since they are not allowed to give any sort of legal advice. Their job is merely to give you the forms requested. With this in mind, I showed up at the court clerk's office with all the information pertinent to my case, and explained that I needed a Warrant in Debt for small claims court (usually called a court summons). I explained that under the statute this company owed me $800 plus my court fees. The clerk was a bit confused, since she did not realize an individual could take a corporation to small claims court. I was a bit baffled, since the court's Web site said that in fact I could. After arguing for a few minutes, I eventually went home to print out the Web site.

I returned with a hard copy of the page and also went one step further and printed out the section of state code that corroborated it. I then proceeded to fill out the proper forms and pay the court fee. Next, I wrote up a settlement letter and attached it to a copy of the summons (so that they would know I was serious). Again, I never received a response from the defendant.

On the date of the trial, I printed out all my communications with Etracks.com (my cease-and-desist letter as well as the settlement letter), the abbreviated headers for all messages received (rather than the full messages, I printed out the To, From, Subject, Date, and Received headers), and, finally, since it was my first time in court, I decided I should write up my testimony. When I got there, I ended up having to wait for about an hour before my case was heard. When it was, the judge was a bit surprised; this was apparently the first spam case he had ever heard. I explained a little bit about the problem, he asked a few questions, and since I had more than enough evidence and the

defendant failed to show up, I was awarded judgment for $841 ($800 for the original complaint, $41 for the court costs).

Send Lawyers, Guns, and Money

Since then I have been filing suits every few months. This is always preceded by a letter sent to the defendant. Last August I received a call from a man who identified himself as Brian Benanhaley, COO and in-house counsel for SubscriberBase, Inc. I had just filed suit against them for 47 messages and they had apparently just received their court summons. This was nothing new; I had been through this routine before – they call, threaten, and then don't follow through. I was expecting the same thing, to receive another default judgment. After just finishing the routine "we're not going to settle, so you better drop your suit since we're not at fault," Mr. Benanhaley went on to threaten to countersue. Having not wanted to really continue this conversation, I told him that he should consult my attorney.

My roommate's parents have a law firm in town, Snook & Haughey P.C., and while his parents did not seem very interested in my spam endeavors, one of the other attorneys in their firm did. He mainly practices business and consumer protection law; he had never done anything like this before and so was very interested in trying some of these cases. Being a poor college student, I had no intention of retaining anyone, but since he was interested in trying to make some case law (our research showed that no cases under the Virginia anti-spam statute had ever been appealed, so we were both hoping for an appeal so that we could set a precedent), he was willing to take the case on contingency.

My attorney, Jim Garrett, seemed to think that SubscriberBase was very serious; they had apparently retained a local firm. My only concern now was that the case was not as straightforward as my others. In Virginia, it is illegal to "falsify or forge header or routing information in any matter." The messages I received all came from seemingly random usernames, though the domains were registered to SubscriberBase. Replies to the messages would bounce. However, the defendants alleged that since they owned the domain names, this does not violate the law. I wanted a judge to make that decision.

In the weeks approaching the trial, the saga became odder and odder. When SubscriberBase first contacted me, they kept insisting that they would be filing a countersuit in their state of South Carolina. Jim insisted that there would absolutely be no merit to any suit that they would bring; I hadn't done anything wrong. They might allege that this was a frivolous suit, but he said that would also be without merit since they continued to spam me even after I had sent them a clear cease-and-desist letter. Each week they would call with a new empty threat; they were still making a counterclaim, this time in Virginia. Next they said that they wouldn't make a counterclaim but would ask the judge for their fees. A week or so before the trial, they called Jim asking if I would be willing to pay their legal fees. He said that he asked them to repeat that, since he was sure he misunderstood. In fact they were indeed asking if I would voluntarily pay for their expenses. You can guess our response.

The fact that I had a lawyer was a fairly big surprise for them. They were in for a few more surprises. I had recruited two volunteers from the Computer Science Department to testify as expert witnesses: a professor and the system administrator. In addition to going through the department's mail logs and finding spam sent by SubscriberBase, we made another huge discovery the day before the trial. I had not noticed this earlier, but the X-Mailer header was clearly forged on all of the messages.

The 47 messages claimed to have been sent from 29 different mail clients running on 11 different platforms (including Amiga). This clearly qualified as "falsified in any manner." We made a printout of all the X-Mailer headers to be entered into evidence during the trial.

On the day of the trial, we met at the law firm to make our final plans. It turned out that my roommate's father, Lloyd Snook, a criminal defense lawyer, would be doing the cross-examinations and the closing arguments. The five of us arrived at the courthouse, and met the opposing four in the hallway (their COO/counsel, CEO, a technical person who didn't look any older than 15, and their local retained counsel).

We decided to call their CEO, Jeff French, first. He answered a few questions about what his company does, his role, their business model, etc. Then he explained in detail what systems they use: a cluster of Linux servers sending out messages via RoboMail (a commercial mass-mailing package). Finally, he explained how they obtain addresses: They purchase lists from other companies of addresses that are "confirmed opt-in."

It was then my turn to testify. I explained how I am a student and run my own server which provides email and Web hosting and that I receive an inordinate volume of spam. I explained that when I register on various sites, I try to do a fairly good job of reading privacy policies and never register for sites that outright say they will sell my personal information. I also create aliases to help in determining where spam is coming from (and which sites are violating their privacy policies).

During my cross-examination, Mr. Benanhaley listed a few sites, asking if I had been to any of them. I had heard of one and explained that I have tracked a lot of spam to that site. I also explained that the defendants had sent spam to three different addresses of mine. It was clear to the court that they make no effort to confirm that each address has really opted in. Finally, I was asked what I was discussing with a friend in the hallway prior to the trial.

Recently I have been working with a group of friends on an idea for a cryptography-related startup and was discussing this outside the courtroom; I guess they must have overheard me. Because we are currently working with another lawyer on a related patent, I really did not want to divulge too many details. So I glanced over at my lawyer, and responded, "I'm sorry, but I really don't see how this is relevant."

"Please just answer the question," said the judge. "If there are objections, your legal team will raise them."

"Objection, your honor. Relevance?"

"Sustained."

The defense then approached the bench and began explaining to the judge how I was committing barratry and that this case was entirely without merit. He went so far as to pull out printouts of slides that were posted on our UNIX User's Group Web site; I had given a talk a few months earlier on current trends in anti-spam tools as well as anti-spam legislation. Most of the people in the audience (in addition to my legal team) were now giggling, since we all knew what I was really talking about and that the defense was really grasping here.

The judge sounded very annoyed; they argued back and forth for what seemed like 10 minutes. I changed my mind and interjected, "If you want, I can just answer." My lawyers shut me up; they were having fun watching the judge lecture the opposing

The 47 messages claimed to have been sent from 29 different mail clients running on 11 different platforms (including Amiga).

counsel. The judge ended the argument by saying, "Regardless of the plaintiff's motivations, we are here to determine if you have violated the law."

After another hour or so of testimony (both my witnesses testified that these messages contained falsified information, though we were still only arguing about the addresses in the From line), we took a recess.

The defense called their CEO and asked that he be an expert witness. My legal team objected after it became clear that his experience was limited to his role as CEO of SubscriberBase. The judge agreed; he could only testify based on his own experiences. During the cross-examination, we asked him why they use the randomly generated From addresses. He explained that "anti-commerce" individuals use various filters to stop spam, and thus the company's "legitimate" advertisements often get filtered out by accident; therefore they take measures to get past such filters.

With this statement, he had admitted that they intentionally format messages to evade filters in order to increase their profit; it was time for the coup de grace. "You testified earlier that you exclusively use RoboMail under Linux to send messages. Why is it that there's no identifier corroborating that in these messages?"

"The same reasons I just mentioned."

"Then maybe you can explain why 29 different mail programs are listed," my lawyer said and handed the list to the CEO, "and why there are also 11 different operating systems mentioned here. Was it not your earlier testimony that you used Linux exclusively?"

Everyone on the defense team suddenly turned bright red. They knew it was over. Half the courtroom was giggling. Mr. French finally responded, "I'm not a technical person, so I'm not entirely positive what we use, come to think of it."

"Well let's just go through the list then." My lawyer began naming off everything on the list, without stopping to wait for responses. When he came to the Amiga, he waited. We all wanted the defense to say that they use an Amiga for their spamming.

"It's entirely possible. We might use one. I would have to double check."

Mr. French was finished testifying. We assumed that given the recent humiliation and disqualification as an expert witness, they would not even bother trying to get their technical person to testify. The defense rested. Closing arguments were made. They argued that "clearly" I opted in and that what they are sending was not even spam.

We asserted that, hypothetically, even if I had opted in, the majority of the messages were received after I sent them a cease-and-desist letter (a copy of which was in evidence). Additionally, the court was reminded that the defense had testified that they willfully altered the headers to evade filters.

After four hours of testimony and arguments, the judge spoke. He started by saying that he was "confident that whatever decision is reached, it will only determine which side files the appeal." He, of course, was right. Unfortunately, this was a different judge from my previous cases, and he was not very familiar with the law. He said that the case would be taken under advisement for a week. Outside I commented, "Hopefully, the first thing he does is go home and check his email."

A week passed before Jim called: we won. I was awarded $470 for the spam, $50 for the filing fee, and $5000 in legal fees (*http://www.guanotronic.com/~serge/opinion.jpg*). The

defendants had 10 days to file an appeal; we were confident that they would, and we welcomed it. And they did, the day after the initial ruling was entered into the court record. In Virginia, when a defendant appeals a civil case, they must also post a bond for the amount awarded to the plaintiff. They had 30 days to do this, but failed. Thus the appeal did not occur and the saga came to an end.

So You've Won a Judgment

I have since been to court about half a dozen times, and have yet to lose a case, though I have only had one spammer show up. Since my first time in court, the judge seems to have gotten friendlier and more interested in what I am doing. No one likes spam; judges receive it too. I am currently owed a little over $5000, but being owed money is quite different from actually receiving it. However, there are legal methods that can be used to aid in the collection process.

The first thing that should be done is to put the judgment on file in a court of record; in most cases, this will be a court above the small claims court (in Virginia, for instance, small claims is part of the general district court, and the court of record is the state circuit court above that). This means that creditors and anyone else with an interest in your debtor will be able to readily see that you are owed money, and this can adversely affect their credit rating.

Once the appeals period is over, various legal means can be used to enforce your judgment. Most of these, however, will only work if the defendant resides or owns property in the state of the judgment. If they do, the first thing that you must do is locate their assets and property; this is done with a Summons to Answer Interrogatories (again, this might be called something else in other states), which means they must show up in court to answer your questions.

If they own real estate, you can place a lien on it (so that your judgment must be satisfied before they can sell the property). If they own other personal property (or property belonging to the business), you can get a Writ of Fieri Facias (sometimes called a Writ of Execution) to have their property sold at public auction. Finally, you can get a Garnishment Summons to garnish their wages or any bank accounts that they have. In any case, you will probably end up the winner (also, all costs incurred during collection can be added to the judgment in most states).

If your debtor resides in another state, there is still hope. You can have the judgment domesticated to the debtor's home state. This means the judgment goes on file with a court there and becomes legally binding in that state. You can then use the measures mentioned above, assuming they are applicable in the new state. To domesticate a judgment; usually, all that is involved is sending a certified copy of the original judgment along with a court fee.

I personally have been going a step further and using a collection agency. Their job is to keep contacting the debtor until they are willing to pay. Collection agencies usually work on contingency and will take anywhere from 30 to 50% of the total amount collected. I use Dun and Bradstreet Small Business Solutions (*http://sbs.dnb.com*), which has another advantage: They are the largest business credit reporting company. This means that when a company is not cooperating with the collection process, their credit report will be adversely affected.

If you do not have the time to try collecting the judgment on your own, using a collection agency is probably the easiest solution. The only disadvantage is that it can take a

long time before you see any money. I just received my first check from the agency for around $400 after three months, care of Mr. Joshua Baer of Skylist.net (I was owed $631 before the commission). For those short on time or energy, there is still one other option: selling the judgment. There exists a market for court judgments: an individual or corporation will give you a fraction of the judgment's value in exchange for the right to collect on it. It won't be much, but it's something and you will receive it quickly.

Conclusion

While I do not think I have personally made an impact on the spam problem, I have certainly helped to decrease the amount I have been receiving. Most have stopped sending me messages after being served with their court summons, though with one company it took three judgments before they got the message. The majority of states have laws that can be exercised by any resident, but such laws are useless unless they are used. The same applies to the newly enacted federal law. Spammers are not going to be deterred by the laws until more individuals begin to take action.