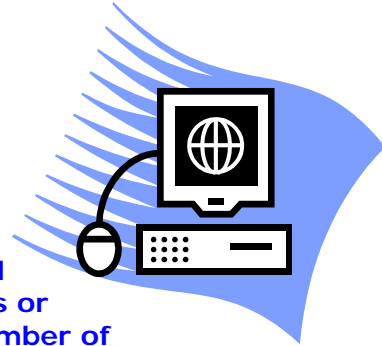


SELLING YOUR NAME TO SPAMMERS: A CRIME

THE PROBLEM:

There are Thirty Two Million names in the coffers of America On Line (AOL) and those names are worth millions to a new industry that has become the plague of all who have access to the Internet: "Spammers." Now it is revealed that **ninety two million screen names** of customers of AOL were sold by an employee of AOL to spammers. (Many families or businesses have multiple screen names thus the number of customers is less than the number of names.)



Spam is defined loosely as unsolicited and unwanted e mail that arrives in a mail box of a user of the internet. All of us have it, all of us hate it...and it is increasing at such a level that it is actually threatening the future of the internet.

Above all the internet is useful for quick and inexpensive access to communication and information. When one opens one's mailbox and finds fifty unwanted messages that must be erased or could be offensive each day, the utility of that tool becomes questionable. Many people report hundreds of spam received each day and the anti spam programs, both expensive and of limited use, cannot overcome the ability of spammers to alter their addresses by small amounts to evade the programs.

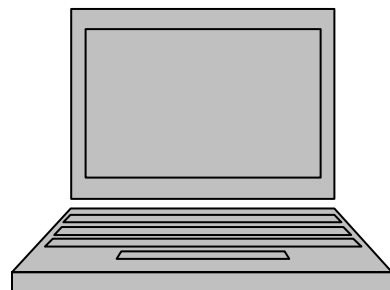
People used to think that if they avoided certain "questionable" web sites that they would be free of spam since the spammers normally get names from visitors to such web sites.

Dream on...

Your screen name, it is now revealed, is a commodity to be sold and your use of AOL or YAHOO or any of those services may expose you to the danger of becoming submerged in the spam that is quickly clogging the arteries of the internet.

CAN THE LAW FIX IT?

The leaders of the internet industry (Microsoft, Yahoo, etc, etc.) are well aware of the danger and have not only sought technological innovations to solve the problem but have pressured Congress to pass anti Spam laws which make it dangerous



for those who engage in or assist Spammers.

The law is only a year old and there are older laws that could be brought to bear but the problem is that much of the harm is perpetrated outside the limits of the United States in nations in which the ability of the United States government to enforce our laws is limited or nonexistent. The former Soviet republics, nations in the Middle East, Asia or Africa can as easily create and impose Spam as a software engineer in Detroit and the United States Attorney has virtually no chance to stop such activities if they emanate from any of two dozen such nations.

Which is why a violation that is capable of prosecution...one involving AOL...has been seized upon by the U.S. Attorney in New York to both make an example and demonstrate vigilance.

But few feel that the case, which will garner much publicity, will really solve the problem for the simple reason that as with so much of the Internet, if we cannot effectuate international laws that are enforceable, we are doomed to fail legally.

FACTS ALLEGED:

Jason Smathers, 24, has been charged with conspiracy to violate the new Anti Spam law and is accused of stealing ninety two million customer screen names that were ultimately utilized to send massive amounts of e mail spam. Smathers, residing in West Virginia, worked at AOL in Virginia and stole the list and sold it to a Las Vegas contact, Sean Dunaway, who utilized it himself to promote an Internet gambling operation and then sold it to other spammers. Sunaway, 21, was arrested and charged with the same conspiracy.

Each suspect faces up to five years in prison and a minimum of two hundred and fifty thousand dollars in fines if convicted.

How did this happen?

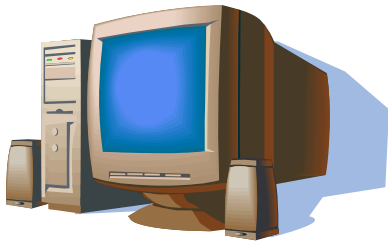
According to the Federal prosecutors, Smathers was not authorized to have access to the screen name list but used another employee's access code to steal the list a year ago. The list also included customer ZIP codes, credit card types, etc. While AOL claims that Smathers did not gain access to credit card numbers (kept in a separate facility by the Company) that is by no means certain. AOL has just terminated Smathers.

While the amount paid to Smathers originally is unknown, an updated version of it sold later was worth one hundred thousand dollars to Smathers. Dunaway then resold the list to spammers, charging them two thousand dollars for lists containing names beginning with a single letter of the alphabet or fifty two thousand dollars for the entire alphabet.

At least one company selling "penile enhancement pills" was one of the buyers.

Which means that for millions of people, including, probably you, the spam arrived on your screen whether you visited a "questionable" site or not. And those names are still out there.

And if you think this is an isolated event...you are wrong. A software engineer over a decade ago told the writer the following: "Go on the Internet and your identity is compromised. Period. It's only a question of what that means..."



THOUGHTS...

Due to the international nature of the internet, all that the Federal government can do is seek to prosecute those within the United States who commit a crime. But let's assume that the culprit worked at AOL, took the list and moved to Libya or Lebanon, Nigeria or Khazatstan, China or Burma. The relief would be nil.

And the danger is acute. It would take only a few sales such as the above to flood your computer with a thousand e mails a day-enough to drive you from the internet world that has become a huge part of your life.

The solution? Either effective international control of the internet is achieved (doubtful in the extreme with such countries as North Korea and Iran) or the same people that brought you the internet will have to develop technological anti spam methods that actually work. And the race is on, as they very well know: either the legitimate businesses on the internet find a way to stop SPAM soon or the spammers will drive people away from this powerful tool.

As for the courts? They can do a little and will-but the courts did not invent the internet and it is clear that they cannot save it...
