

Recent Legal Developments in CyberCrime & Terrorism

Gary Rogers

Assistant Professor

Jason Ashford

Asst. District Attorney, Houston County, Georgia

Macon State College

100 College Station Drive

Macon, GA 31206

(478) 471-2809

grogers@mail.maconstate.edu

Introduction

Congress and individual states have been busy over the past year combating spam, protecting (or eroding, depending on your perspective) privacy rights, and trying to catch the law up with the cyber criminal. This paper will examine recent legislative developments in the above titled areas of spam, privacy, and cybercrime from both Congress and state legislatures, and will also briefly discuss current initiatives that have failed to pass but could represent possible trends in these areas.

The Computer Security Institute (CSI) conducts a survey in association with the FBI annually to examine the current state of cybercrime and its effects. The latest report, the 2003 CSI/FBI Computer Crime and Security Survey, looks at several hundred companies, big and small, and asks about intrusions, loss, and attitudes and responses to computer crime.

The report states that losses from computer attack fell 57 percent from record levels last year, mainly in the areas of computer fraud. While unauthorized use was about the same at approximately 60 percent, computer fraud losses from survey respondents fell dramatically from \$116 million last year to just \$10 million. Theft of proprietary information remained the number one area of survey respondent loss from attack, but denial of service attacks were a close second. The most common forms of attack remain virus attacks, with insider abuse of network access slightly behind. As an interesting side note, respondents continued to be against hiring reformed hackers as security consultants and only 30 percent of those respondents reporting security intrusions reported them to law enforcement.

Clearly, though the number of security incidents remained essentially unchanged, the dramatic drop in computer fraud may show that high profile prosecutions of these crimes may be acting as a deterrent for the potential perpetrator, or that precautions by industry are catching up to the cyber criminal and helping to minimize the damage done per intrusion.

Another form of intrusion that has the average citizen calling their congressperson is spam, or unauthorized email. Perhaps no other aspect of the internet is so universally hated that the dreaded spam message hawking the latest pill, potion, or plan to get rich. According to a new study published on January 6, 2002 by market researcher Ferris Research, the annual cost of spam to U.S. corporations is \$8.9 billion, and \$2.5 billion for European businesses. U.S. and European service providers take on an additional \$500 million in costs due to spam. Individual

states have attempted to regulate this menace, businesses have resisted plans to mandate toll-free lines to opt-out of mailings, and Congress has been debating the merits of several plans for some time. The courts have ruled at least two state laws against SPAM unconstitutional because they were "unduly restrictive and burdensome", and Congress searched for some time to develop a law that balanced the free speech rights of the advertiser with the privacy and property rights of the consumer and Internet Service Provider. Congress and President Bush signed the "Can-Spam Act of 2003" and it went into effect at the beginning of 2004.

Spam Legislation

The Can-Spam Act of 2003, officially called the Controlling the Assault of Non-Solicited Pornography and Marketing Act, requires unsolicited commercial e-mail messages to be labeled as such.

The Act also required the advertiser to include opt-out instructions and the sender's physical address. Obviously this is problematic to enforce since most spam comes from email domains that either don't exist or are used without permission. Subject lines and headers in messages that are deceptive are prohibited, but no definition of specific deceptive practices is mentioned in the act, leaving the courts to shape this area. Finally, the Federal Trade Commission is authorized but not mandated to establish a "do-not-email" registry, similarly to their widely popular do-not-call for telephone solicitation.

Previous state laws, such as California's, that require the subject line of any unsolicited email to start with "ADV" would be preempted or superseded by the Can-Spam Act, as would any state or local laws that regulate opt-out procedures. State laws prohibiting unsolicited email entirely are also preempted by this act, though such laws were unlikely to pass constitutional muster once they were litigated. State laws are not entirely superseded by this act, however. Any state laws dealing with falsity, deceptive business practices or fraud in these messages would remain in place.

Overall, this law, while sounding tough, appears hold little promise for reducing spam in the future, primarily because it seeks to legislate out what is essentially a technical problem: being able to track the identity of someone sending bulk email on the net, and shifting the costs of their behavior to them rather than the end user and the service provider. Its lack of specifics, like labeling convention for spam, making filtering difficult if not impossible, and its precatory directives to the FTC mean action will be delayed if not avoided.

Hopefully, some of the bills that did not pass that have more enforcement teeth show a trend in Congressional action in the future. The Computer Owners' Bill of Rights, proposed in 2003, would require the FTC to setup a do-not-email list, and provides for the imposition of civil penalties upon those who send unsolicited commercial e-mail to addresses listed on the registry. The Stop Pornography and Abusive Marketing Act, proposed by not adopted in 2003, required specific subject line labeling, assisting in filtering. While both of these proposed bills mandate actions only suggested in the Can-Spam Act, they appear to fall outside anything "unduly burdensome" to advertisers, a requirement under current caselaw.

Finally, perhaps representing the vanguard of spam, the Wireless Telephone Spam Protection Act proposed in January 2003 to prohibit the use of wireless messaging systems to send spam primarily to cellular phones and pagers. While not a major problem yet, spammers are not doubt planning these and other offensives in the future and it is promising to see Congress at least thinking on the cutting edge.

CyberCrime and Privacy Legislative Developments

The Patriot Act, though passed in response to the attacks on the World Trade Center in 2001, is only now being analyzed and examined with sufficient detail to raise the ire of civil libertarians.

The Patriot Act, whose lengthy and official title is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, has been analyzed in great detail by both proponents and detractors. The Act consists of ten titles which, among other things: give federal law enforcement and intelligence officers greater authority to gather and share evidence particularly with respect to wire and electronic communications; allowing “sneak and peek” search warrants which don’t require notification of the person or organization searched; amend federal money laundering statutes and make them more restrictive particularly with overseas accounts; changes existing federal criminal procedure, particularly with respect to acts of terrorism; and finally to modifies immigration law, increasing the ability of federal authorities to prevent foreign terrorists from entering the U.S., and to detain and/or deport foreign terrorist suspects.

While clearly the potential for abuse of the act is present, prosecutorial and law enforcement discretion is required with all the laws, and the Patriot Act simply streamlines and facilitates existing laws and procedures.

Civil liberty advocates are also concerned about the potential privacy implications of the Cyber Security Enhancement Act, part of the Homeland Security Act (HSA). Several of the CSEA’s provisions allow Internet service providers to disclose customer information in exigent circumstances without probable cause that the information is linked to a crime. Specifically it states companies can disclose information based on the good faith belief of “an emergency involving danger of death or serious physical injury to any person”. This determination is done by the holder of the information, and could lead to abuses.

Conclusion

While much of the legislation discussed has the potential to change the cybercrime and privacy law landscape, inertia and the strong and understandable resistance to place burdens on commerce prevents rapid and comprehensive action in the areas of Spam, Cybercrime, and privacy protection.