The Effects of Spyware and Phishing on the Privacy Rights of Internet Users

SARAH A. CHERRY*

ABSTRACT

This article reviews the major events of 2005-2006 in the areas of Spyware, Phishing and Spoofing under the umbrella of Internet Privacy. Spyware issues are troubling to businesses and consumers alike and present the legal community with many challenges, such as balancing the interests of these two groups. Proposed legislation at the state and federal level must carefully define the activities that are to be illegal without outlawing legitimate business activity while not defining illegal acts too narrowly so as to render the legislation ineffective. States that want to handle the problems caused by spyware and phishing activities are put in an awkward position as their legislation may be preempted by a federal standard. Efficient use of government resources in creating this complex legislation is a concern. This article discusses proposed legislation at the international, federal, and state levels as well as federal and state litigation in these areas as these issues are being played out in our courts before our lawmakers can write the playbook. This article does not attempt to chronicle every single event from 2005-2006 related to spyware or phishing but rather aims to identify trends in dealing with these problems and the major legal issues in these areas.

I. SPYWARE

Spyware was again a major problem for businesses and consumers in 2005. The Federal Trade Commission, the nation's consumer protection agency, recognizes that spyware is a nebulous term for invasive, uninvited software. However, the FTC attempts to define spyware loosely as a program installed without the user's consent that performs tasks such as sending pop-up ads, redirecting a computer to bogus web sites, usage monitoring, and keystroke recording.[1]

---

* The author is a J.D. candidate at The Ohio State University Moritz College of Law, class of 2007. Sarah A. Cherry, B.A., Ohio University, 1998; Consultant, Computer Associates, 1998 - 2004.

[1] Federal Trade Commission, *FTC Consumer Alert: Spyware*, July 2005, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.pdf (alerting consumers of the warning signs that spyware is present on their machines and suggesting ways to protect themselves from potential harm). The FTC also described spyware at one of its workshops as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." Spyware

The aspects of spyware that cause the most concern involve installation without notice or consent and intrusion on users' privacy. Imagine if someone were secretly plugging his elaborate holiday light display into his neighbor's electrical supply. The resulting increase in the neighbor's electric bill would be measurable and no doubt vexing to the unsuspecting neighbor. The neighbor's right to use his property as he pleases would be impaired by the sneaky electricity thief. While the effect of spyware is harder to measure in dollars, it results in a comparable violation of rights. This analogy only addresses spyware's drain on resources rather than what information is stolen, but that drain is a chief concern of consumers as it costs them time and money. There is nothing new about the observation that people do not like it when their right to use their personal property freely is violated, especially when profits are being made at the expense of the uncompensated victim of spyware.

The term spyware for the purpose of this article sometimes encompasses or is discussed in concert with "adware" and "malware." Malware is short for malicious software, and its only purpose is to harm a user's computer system or Internet experience.[2] Adware is software that displays advertisements to users while the adware program is running.[3] While it is meant to describe a legitimate Internet business tool, adware is cautiously defined by several sources as a type of spyware.[4] The line between spyware and adware is blurry

---

Workshop, 69 Fed. Reg. 8538 (Feb. 24, 2004), *available at* http://www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf. The Anti-Spyware Coalition, in referring to spyware, uses the phrase "spyware and other potentially unwanted technologies" to reflect that the term spyware on its own, having been defined as a term of art by other entities, may not be able to cover all of the potential malicious and invasive spying programs. The Coalition defines spyware and other potentially unwanted technologies as "[t]echnologies deployed without appropriate user consent and/or implemented in ways that impair user control over: [m]aterial changes that affect their user experience, privacy, or system security; [u]se of their system resources, including what programs are installed on their computers; and/or [c]ollection, use, and distribution of their personal or other sensitive information." Anti-Spyware Coalition, *Definitions and Supporting Documents*, http://www.antispywarecoalition.org/documents/definitions.htm (last visited Feb. 13, 2006).

[2] Webopedia, What is Malware?, http://www.webopedia.com/TERM/m/malware.html (last visited Feb. 13, 2006).

[3] Webopedia, What is Adware?, http://www.webopedia.com/TERM/a/adware.html (last visited Feb. 13, 2006).

[4] *Id.* Dictionary.com, http://dictionary.reference.com/search?q=adware (last visited Feb. 13, 2006). "[S]ome freeware applications which contain adware do track your surfing habits in order to serve ads related to you. When the adware becomes intrusive like this, then we move

and Internet advertisers will have to comply with laws governing spyware distribution to ensure they are on the right side of that line. The definition of spyware is still being refined by many different parties, so the term can mean different things to different people.

Another phenomenon that gained attention in 2005 was the threat to privacy posed by some companies claiming to be part of the anti-spyware industry. With the proliferation of spyware and the public's growing fear and aggravation with it, opportunists poised themselves to exploit that fear. Several supposed anti-spyware companies were found to have behaved fraudulently in the marketplace.[5] The anti-spyware movement can boast some successes in its self-policing efforts but at least one of these efforts failed in 2005. The Consortium of Anti-Spyware Technology vendors ("COAST"), one of the industry groups formed to combat spyware by identifying standards for anti-spyware vendors to use, dissolved due to potentially competing interests among members.[6]

In 2005, two pieces of federal legislation on spyware from 2004 were reintroduced and several new bills were introduced. All of the bills found their way to Senate committees for consideration but none had passed by the conclusion of the year. There is concern among experts that the approach to legislating spyware is too piecemeal to be very effective in protecting citizens' privacy. The proliferation of state legislation involving spyware in 2005 adds to that concern as businesses and consumers now have to deal with different standards among different states. The states' laws could be rendered moot by preemptive federal legislation in 2006.

Progress was made in key cases from 2004 involving spyware and new cases were prosecuted as the federal courts were once again

---

it in the spyware category and it then becomes something you should avoid for privacy and security reasons. Due to its invasive nature, spyware has really given adware a bad name as many people do not know the differences between the two, or use the the terms interchangeably." Vangie 'Aurora' Beal, *The Difference Between Adware and Spyware*, Webopedia, Nov. 11, 2004, http://www.webopedia.com/DidYouKnow/Internet/2004/spyware.asp.

[5] Press Release, Federal Trade Commission, Two Bogus Anti-spyware Operators Settle FTC Charges (Jan. 5, 2006), http://www.ftc.gov/opa/2006/01/maxtrust.htm. [hereinafter *Bogus Anti-Spyware*].

[6] John Leyden, *Anti-Spyware Group Collapses*, THE REGISTER, Apr. 13, 2005, http://www.theregister.co.uk/2005/04/13/coast_collapse/.

forced to navigate uncharted waters in the absence of legislative guidance. This article discusses 2005 developments in federal and state litigation in the spyware arena. This article also discusses developments in international law involving spyware and how such developments will impact spyware legislation in the United States.

All of this attention to spyware may have resulted in the decreased presence of spyware on consumers' computers in 2005. An America Online/National Cyber Security Alliance study found that the percentage of computers with spyware on them decreased to 61% in 2005, down from 80% in 2004. The study also found that 62% of computers had anti-spyware software installed.[7] The Center for Democracy and Technology also credits increased enforcement actions for this decrease.[8]

A. FEDERAL LEGISLATION

Toward the end of 2005, there were five pieces of federal legislation in committee regarding the regulation of spyware. The Internet Spyware Prevention Act of 2004 ("I-SPY") and the Spy Act of 2004 were reintroduced in 2005 as the I-SPY Act of 2005 and the Spy Act of 2005.[9] Both bills originated in the House and were referred to the Senate Committee on Commerce, Science, and Transportation in May, 2005. Three new pieces of spyware legislation were introduced in the Senate in 2005: the SPY BLOCK Act, the Enhanced Consumer Protection Against Spyware Act of 2005 ("Enhanced Act") and the U.S. SAFE WEB Act of 2005.[10]

---

[7] Center for Democracy and Technology, *Study Finds Decrease in Spyware*, Dec. 7, 2005, http://www.cdt.org/headlines/840; AMERICA ONLINE AND THE NATIONAL CYBER SECURITY ALLIANCE, AOL/NCSA ONLINE SAFETY STUDY, (Dec. 2005), *available at* http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

[8] *Id.*

[9] I-SPY, H.R. 744, 109th Cong. (1st Sess. 2005). Spy Act, H.R. 29, 109th Cong. (1st Sess. 2005).

[10] SPY BLOCK Act, S. 687, 109th Cong. (1st Sess. 2005); Enhanced Consumer Protection Against Spyware Act of 2005, S. 1004, 109th Cong. (1st Sess 2005); U.S. SAFE WEB Act of 2005, S. 1608, 109th Cong. (1st Sess. 2005). All three bills were referred to the Senate Committee on Commerce, Science, and Transportation. The SPY BLOCK Act has been placed on the legislative calendar of the Senate as of June 12, 2006. A different version of the SPY BLOCK Act was reported in the Senate committee.

The Senate approved the SPY BLOCK Act, setting it up for potential passage in 2006.[11] Compared to other proposed bills, this Act is focused more on protecting consumers from intrusive, malicious invasions of privacy and drains on computer resources by spyware than some of the other proposed bills. The Enhanced Act, alternatively, is considered to be more pro-business. It is not as detailed as the SPY BLOCK Act in defining what acts are illegal.[12] The Enhanced Act does not even contain the word "adware" whereas, with regard to adware that may conceal its operation, the SPY BLOCK Act provides:

> (a) IN GENERAL- It is unlawful for a person who is not an authorized user of a protected computer to cause the installation on that computer of software that causes advertisements to be displayed to the user *without a label or other reasonable means of identifying* to the user of the computer, *each time* such an advertisement is displayed, *which software caused* the advertisement's delivery.
>
> (b) EXCEPTION- Software that causes advertisements to be displayed without a label or other reasonable means of identification shall not give rise to liability under subsection (a) if those advertisements are displayed to a user of the computer--
>
> (1) *only* when a user is accessing an Internet website or online service--
>
> (A) *operated by the publisher of the software*; or
>
> (B) the operator of which has provided *express consent* to the display of such advertisements to users of the website or service; or

---

[11] Caron Carlson, *Senate Panel Approves Data-Breach Bill*, EWEEK, Nov. 21, 2005, http://www.eweek.com/article2/0,1895,1891550,00.asp.

[12] Enhanced Consumer Protection Against Spyware Act of 2005, S. 1004, 109th Cong. (1st Sess. 2005).

> (2) only in a manner or at a time such that a *reasonable user would understand which software caused the delivery* of the advertisements.[13]

The SPY BLOCK Act, in Sections 2-5 of the bill, outlaws the following:

1. "Surreptitious Installation" including concealed installation or installation without consent, "misleading inducements to install," and "preventing reasonable efforts to uninstall;"

2. Installation of "surreptitious information collection features" defined as software features that collect and transmit information that the authorized user has not triggered and that have not notified the authorized user of the type of information to be transmitted or provided an opportunity for the user to stop the transmission;

3. "Adware that conceals its operation" as noted above; and

4. "Other practices that thwart user control of computer" such as displaying an excessive number

---

[13] S. 687, 109th Cong. § 4. (1st Sess. 2005). The reported version of the SPY BLOCK Act (S. 687, 109th Cong. (2d Sess. 2005)) contains the following revisions to § 4 (denoted as "§ 104" in the reported version):

(a) IN GENERAL.— It is unlawful for a person who is not an authorized user of a protected computer to cause the installation on that computer of software that collects sensitive personal information from an authorized user, unless that person provides a clear and conspicuous disclosure of such collection and obtains the authorized user's consent prior to any such collection of information in any case in which the software extracts from the hard drive or other storage medium of the protected computer the authorized user's— (1) Social Security number; (2) tax identification number; (3) driver's license number; (4) passport number; (5) any other government-issued identification number; (6) financial account, credit card, or debit card numbers; (7) account balances, or overdraft history; or (8) other sensitive personal information. . . . (c) EXCEPTION.— This section shall not be interpreted to restrict a person from causing the installation of software that collects information for the provider of an online service or website knowingly used or subscribed to by an authorized user if the information collected is used only to affect the user's experience while using the online service or website.

> of pop-up advertisements that causes the user to have to shut down their machine to get rid of them or directing the user's Internet browser to a website not intended to be viewed by the user.[14]

The SPY BLOCK Act also takes the extra step of outlawing third-parties' knowing authorization of others to use spyware programs to push ads or monitor activity for the third party.[15] This will likely pressure companies to advertise responsibly and help curb the cash flow to unscrupulous spyware providers.

One key difference between the two bills is that the Enhanced Act explicitly denies a private right of action to the public while providing that state attorney generals may bring civil suits and collect damages on behalf of the public.[16] State attorney general action is precluded however, where the U.S. Attorney General takes action against a violator of the Enhanced Act.[17] Under the SPY BLOCK Act, state attorney generals can bring action and recover actual damages for citizens but the Act does not expressly deny a private right of action or simultaneous state attorney general action where the U.S. Attorney General has stepped in.[18] This difference would seem to make the Enhanced Act more palatable to businesses.

The SPY BLOCK Act differs from the Enhanced Act in its detailed specification of bad acts that will result in criminal penalties or civil damages, but the two bills do share similarities.[19] The Enhanced Act and the SPY BLOCK Act both contain sections on

---

[14] S. 687, 109th Cong. §§ 2-5 (1st Sess. 2005). Section 103 of the version of this bill which was reported in the Senate does not contain the specific term "surreptitious installation," but includes similar language in § 103 and § 104 prohibiting the unauthorized installation of personally identifying information.

[15] *Id.* at § 6; the reported version of the bill contains this provision in § 106.

[16] S. 1004, 109th Cong. § 5 (1st Sess. 2005).

[17] *Id.*

[18] S. 687, 109th Cong. § 9 (1st Sess. 2005); The reported version of the SPY BLOCK Act contains the provision regarding state enforcement in § 109.

[19] S. 687, 109th Cong. § 12 (1st Sess. 2005); The reported version of the SPY BLOCK Act contains the provision regarding criminal penalties in § 113.

limiting liability of law enforcement, for example.[20] The Enhanced Act exempts from liability investigational activities that are accompanied by some kind of warrant or court order while the SPY BLOCK Act exempts "lawfully authorized" enforcement activity.

Both acts focus on the FTC's power to bring enforcement actions against those who would use unfair or deceptive practices to harm consumers; the SPY BLOCK Act contains a section explicitly allowing the FTC to make rules to implement this act.[21] The Enhanced Act does not grant this authority explicitly but implies that the FTC already has this rule-making power and notes that violations of the Act or its implementing rules will be treated as violations of the FTC Act's prohibition on unfair or deceptive trade practices.[22]

With regard to preemption, both the Enhanced Act and the SPY BLOCK Act would preempt state laws that govern spyware. The Enhanced Act provides as follows:

> (e) Preemption of State or Local Law- This section supersedes any provision of a statute, regulation, or rule, and any other requirement, prohibition or remedy under State law or the law of a political subdivision of a State that relates to or affects installation of software through deceptive acts or practices or the use of computer software installed by means of the Internet.[23]

The SPY BLOCK Act provides a more detailed preemption section and is careful not to step on the toes of traditional state laws governing such things as tort and contract disputes:

> (1) STATE LAW CONCERNING INFORMATION COLLECTION SOFTWARE OR ADWARE.— This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly limits or

---

[20] S. 1004, 109th Cong. § 6 (1st Sess. 2005); S. 687, 109th Cong. § 6 (1st Sess. 2005); The reported version of the SPY BLOCK Act contains this provision in § 106.

[21] S. 1004, 109th Cong. § 5 (1st Sess. 2005); S. 687, 109th Cong. § 7 (1st Sess. 2005); The reported version of the SPY BLOCK Act contains this provision in § 107.

[22] S. 1004, 109th Cong. § 9 (1st Sess. 2005).

[23] *Id.* at § 5.

> restricts the installation or use of software on a protected computer to—
>
> (A) collect information about the user of the computer or the user's Internet browsing behavior or other use of the computer; or
>
> (B) cause advertisements to be delivered to the user of the computer, except to the extent that any such statute, regulation, or rule prohibits deception in connection with the installation or use of such software.
>
> (2) STATE LAW CONCERNING NOTICE OF SOFTWARE INSTALLATION.— This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that prescribes specific methods for providing notification before the installation of software on a computer.
>
> (3) STATE LAW NOT SPECIFIC TO SOFTWARE.— This Act shall not be construed to preempt the applicability of State criminal, trespass, contract, tort, or anti-fraud law.[24]

Preemption of the state spyware laws will be one of the most important effects of passing federal legislation. One uniform standard with which to comply will be welcomed by businesses, as most players in the software industry compete in multiple states and are now facing the burden of complying with at least twelve state laws with varying levels of restriction.[25]

A major concern in legislating spyware and other intrusive technologies involves the danger of defining the illegal programs and acts too specifically thereby allowing bad actors to narrowly escape classification as violators of the laws.[26] Ari Schwartz is currently the

---

[24] S. 687, 109th Cong. § 10 (1st Sess. 2005). The reported version of the SPY BLOCK Act contains similar provisions in §§ 110-111.

[25] For the list of states, see National Conference of State Legislatures, *infra* note 37.

[26] "[Anti-Spyware legislation] will be a positive development if the legislation . . . [r]emains technology-neutral, i.e. proscribes 'bad behaviors' instead of specific technologies." The X Lab is a private company that provides Mac OS X troubleshooting and other services to its

deputy director for the Center for Democracy and Technology, a group in Washington D.C. that advocates for the preservation of the right of privacy in the digital age.[27] In response to the Senate's approval of the SPY BLOCK Act before the year's end, Schwartz asked, "Where does it stop if you keep doing this sectorally?," voicing the opinion of many that a broader privacy law should be enacted instead of wasting time on technology-specific bills.[28] There is additional concern that the Senate and House with their seventy and sixty day respective work calendars for 2006 will not have time to enact legislation involving these technological threats to privacy, especially given that it is a mid-term election year.[29]

Additionally, one has to consider the actual necessity of new federal legislation.[30] While it will preempt the patchwork of state spyware laws that have cropped up and provide a uniform standard for businesses, an enforcement problem remains.[31] As the Enhanced Consumer Protection Against Spyware Act of 2005 emphasizes, the

---

customers. The X-Lab, *Spyware Legislation in the United States*, (2005), http://www.thexlab.com/faqs/usspywarelaw.html.

[27] Center for Democracy and Technology, *About Us*, http://www.cdt.org/about/ (last visited Feb. 13, 2006).

[28] "Some privacy advocates and some in industry are urging Congress to enact a broader privacy law rather than addressing the matter on a technology-specific basis." Carlson, *supra* note 11.

[29] Elizabeth Wilner, Mark Murray and Huma Zaidi, *First Read – the Day in Politics*, MSNBC.COM, Jan. 18, 2006, http://firstread.msnbc.msn.com/.

[30] "It's not clear, though, how much a new federal law can accomplish. The Can-Spam Act of 2003 hasn't exactly eliminated junk email so far, and both the FTC and the Justice Department say they already have the power to investigate and punish the worst offenders. Also, no US law can hope to reach offshore websites." Declan McCullagh, Senate Pledges to Get Serious About Spyware, SILICON.COM, May 12, 2005, http://management.silicon.com/government/0,39024677,39130336,00.htm.

[31] "A patchwork of conflicting state laws, particularly as they define spyware, could create a compliance nightmare for spyware developers and marketers alike. Another solution would be for industry members to join with federal legislatures, as they did with CAN-SPAM, to create a carefully worded preemption law that regulates the abusive aspects of spyware, leaving legitimate software use untouched." Michael Barkow, *Spyware Under Attack*, International Association of Privacy Professionals https://www.privacyassociation.org/index.php?option=com_content&task=view&id=216&Itemid=125 (last visited Feb. 13, 2006). The International Association of Privacy Professionals has over 2,000 members comprising privacy professionals from the private, public, and government sectors.

FTC arguably has enough authority already to prosecute violations of the Federal Trade Commission Act's prohibition on unfair or deceptive acts.[32]

Legislation is not the only way to reign in the harms of spyware. The market is somewhat self-policing because businesses have an incentive to look for ways to lower costs and to capitalize on consumers' desire to rid themselves of spyware. Industry groups that advocate certain legislation and federal advisory boards that devise policy and make recommendations to lawmakers have formed in recent years. The Anti-Spyware Coalition is one of these groups whose mission is "building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies."[33]

However, problems arise when the potential perpetrators of privacy invasion are invited to join these groups and panels. For example, the Consortium of Anti-Spyware Technology disbanded in early 2005 when the goals of the individual members seemed to be in conflict.[34] 180Solutions became a member of the group, and other members became concerned about an adware maker being on the board alongside those that would oppose some of 180Solutions' practices.[35]

Another surprising member of an anti-spyware panel is Claria which was appointed by the Department of Homeland Security to sit on the Data Privacy and Integrity Advisory Committee.[36] One must

---

[32] *See* 15 U.S.C.A § 45(a)(1) (West 2005).

[33] Anti-Spyware Coalition, *About the ASC*, http://www.antispywarecoalition.org/index.htm (last visited Feb. 13, 2006).

[34] Stacy Cowley, *Coast Antispyware Consortium Falls Apart*, INFOWORLD, Feb. 8, 2005, http://www.infoworld.com/article/05/02/08/HNcoastfallsapart_1.html.

[35] *Id.*

[36] "In the past, Claria's pop-up ad software has riled some users who claimed it was annoying, installed without permission, and not easy to delete." Declan McCullagh, *Adware Maker Joins Federal Privacy Board*, CNET NEWS.COM, Feb. 23, 2005, http://news.com.com/2100-1028_3-5587653.html. Publishers were unhappy with Claria's practice of displaying ads for competitors on their websites. Claria has sought to improve its reputation by changing its methods. For example, the company now offers to display ads based on end user behavior. Stefanie Olsen, *Firm Formerly Known as Gator Looks for Credibility*, CNET NEWS.COM, Feb. 14, 2005, http://news.com.com/Firm+formerly+known+as+Gator+looks+for+credibility/2100-1024_3-5576389.html?tag=nl.

question how honestly and effectively the problems of spyware can be approached and resolved when perpetrators of questionable practices are able to influence the response to these practices. Does allowing the fox to guard the henhouse protect the best interests of consumers? Input from legitimate businesses is necessary and valuable to solving the spyware problem. However, there must be transparency with regard to the motives of private business participants, and their influence should not be disproportionate to that of consumer rights advocates.

B. STATE LEGISLATION

In 2005, twenty-eight states considered legislation involving the regulation of spyware, with twelve states passing laws: Alaska, Arizona, Arkansas, California, Georgia, Indiana, Iowa, New Hampshire, Texas, Utah, Virginia, and Washington.[37] This is a sharp increase from 2004, when only seven states considered such legislation and only two states passed laws relating to spyware.[38]

Utah passed the nation's first anti-spyware law in June 2004. After concerns that the law was too broad, it was enjoined by a Utah state court.[39] An Internet advertising company called WhenU.com

---

[37] National Conference of State Legislatures, *2005 State Legislation Relating to Internet Spyware or Adware*, Dec. 27, 2005, http://www.ncsl.org/programs/lis/spyware05.htm. S.B. 140, 24th Leg., (Alaska 2005). H.B. 2414, 47th Leg., Reg. Sess. (Ariz. 2005). H.B. 2261, 85th Gen. Assem., Reg. Sess., (Ark. 2005). S.B. 355, 2005-06 Sess. (Cal. 2005). S.B. 127, 2005-06 Sess. (Ga. 2005). H.B. 1714, 114th Gen. Assem. (Ind. 2005). H.F. 614, 2005-06 Sess. (Iowa 2005). H.B. 47, 2005 Sess. (N.H. 2005). S.B. 327, 79th Leg., 2d Sess. (Tex. 2005). H.B. 104, 2005 Gen. Sess. (Utah 2005). H.B. 2215, 2005 Sess. (Va. 2005). S.B. 1163, 2005 Sess. (Va. 2005). H.B. 1012, 59th Leg., Reg. Sess. (Wash. 2005).

[38] Iowa, Michigan, New York, Pennsylvania, and Virginia considered laws to regulate spyware in 2004 while only California and Utah passed laws on the subject. National Conference of State Legislatures, *2004 State Legislation Relating to Internet Spyware or Adware*, Jan. 28, 2005, http://www.ncsl.org/programs/lis/spyware04.htm. In 2005, only Virginia and Iowa succeeded in passing a law on spyware while Michigan, New York, and Pennsylvania introduced new legislation but did not pass any. H.B. 2215, 2005 Sess. (Va. 2005). S.B. 1163, 2005 Sess. (Va. 2005). H.F. 614, 2005-06 Sess. (Iowa 2005).

[39] Agreeing with the court's decision to enjoin Utah's law which virtually banned pop-up advertisements, Anita Ramasastry, Associate Professor of Law at the University of Washington School of Law in Seattle and Director of the Shidler Center for Law, Commerce & Technology wrote, "If free content is to persist on the Internet, pop-up ads may be the price that we pay." Anita Ramasastry, *Why A Utah Court Was Right to Hold That, Under Utah Law, Pop-up Ads Are Not "Spam"*, FINDLAW.COM, Jan. 12, 2005, http://writ.corporate.findlaw.com/ramasastry/20050112.html.

sued to have the law's enforcement enjoined, claiming that the law's interference with interstate commerce was unconstitutional and that it infringed on legitimate web business practices.[40] Utah's law, the Spyware Control Act, barred context-based advertising and pop-up advertising even if users consented to the installation of software that performed these functions.[41] Utah passed the 2005 Spyware Control Act, which was practically a complete rewrite of the 2004 bill, excluding the questionable portions involving approved services.[42] For example, the 2004 version of the Spyware Control Act virtually prohibited pop-up ads that were based on any kind of content trigger and would block the web page a user was attempting to view, noting that it was no defense that such an ad could be moved or closed by the user. The 2005 Act does not treat adware with such broad strokes, leaving room for legitimate business practices to be used in the state. At the time of this article, no new lawsuits had been brought to challenge Utah's law.

California actually passed a law regulating spyware in 2004. In 2005, the legislature took action to make phishing practices illegal with the Anti-Phishing Act. The Act will be discussed later in the Phishing section of this article but, with regards to spyware, the Anti-Phishing Act emphasizes that it is a companion to the existing Consumer Protection Against Computer Spyware Act in that the laws share the goal of enhancing Internet security.[43] The California Senate

---

[40] Stefanie Olsen, *Utah Judge Freezes Anti-Spyware Law*, CNET NEWS.COM, June 22, 2004, http://news.com.com/2100-1024_3-5244151.html.

[41] *Id.*

[42] Spyware Control Act, Utah Code Ann. §§ 13-40-101 to 401 (West 2005). Eric Goldman is an Assistant Professor at Marquette University Law School in Milwaukee, Wisconsin with experience as a practicing attorney in the areas of technology transactions and the Internet. Professor Goldman speculated that the 2004 case against the State of Utah is now moot because the law has been rewritten. Posting of Eric Goldman to Technology & Marketing Law Blog, *Utah Amends Spyware Control Act*, http://blog.ericgoldman.org/archives/2005/03/utah_amends_spy.htm (Mar. 22, 2005, 11:00 AM). [hereinafter GOLDMAN BLOG]. *See also* Brice Wallace, *Utah House Committee Sends on Anti-Spyware Bill,* DESERET MORNING NEWS, Feb. 8, 2005, *available at* http://deseretnews.com/dn/view/0,1249,600110414,00.html (Utah Representative Urquhart, discussing how websites of Utah companies like Overstock.com get inundated with competitors' pop-up ads, "likened it to lemonade stands, in which everyone wants competition by having more stands, but pop-ups, he said, 'are stealing lemons off of someone else's tree.'").

[43] S.B. 355, 2005-06 Sess. (Cal. 2005).

also passed a bill that has not yet passed the House that would allow a consumer, an Internet Service Provider, the Attorney General, or a District Attorney to recover damages and attorney fees from one who would violate California's existing spyware law.[44]

Most of the proposed federal anti-spyware legislation have provisions explicitly designating the laws as preemptive of state laws governing the same matters. The SPY BLOCK Act preempts state laws concerning 1) "information collection software or adware" or 2) "notice of software installation."[45] Even though their hard work on spyware legislation will be superseded, the state legislatures that aggressively addressed spyware can be sure that their actions helped speed up the federal response to this problem.

C. INTERNATIONAL LEGISLATION

Australia was the only other nation in 2005 to introduce spyware-specific legislation, but the law did not pass by year's end. Though other countries did not target spyware specifically with new laws, Canada and the European Union did address the problem and demonstrate the need to fight purveyors of spyware.

Australia's bill requires software to give notice and receive user consent before installing on a user's machine; otherwise, the software will be classified as spyware.[46] Electronic Frontiers Australia has

---

[44] The bill was introduced on January 14, 2005 and was amended several times throughout the year, most recently on August 24, 2006. S.B. 92, 2005-06 Sess. (Cal. 2005).

[45] Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), S. 687, 109th Cong. (as reported by the S. Comm. on Commerce, Science, and Transportation, Nov. 17, 2005).

[46] Benjamin Edelman is a well-known expert in the area of Spyware. His website is dedicated to documenting the acts of the top spyware offenders as well as legislation and lawsuits that shape spyware policy at the state, federal, and international levels. Ben Edelman, *"Spyware": Research, Testing, Legislation, and Suits*, http://www.benedelman.org/spyware/ (last visited Feb. 13, 2006). *See also,* Australian Consumers' Association, *Spyware Illegal Under Australian Law*, CHOICE, Apr. 2005, http://www.choice.com.au/viewArticle.aspx?id=104706&catId=100245&tid=100008&p=1 (The Australian Department for Communications, Information Technology and the Arts. (DCITA) has defined spyware as "any software application that is generally installed without the knowledge or consent of the user, to obtain, use or interfere with personal information or resources, content or settings for malicious or undesirable purposes."). The bill had its first reading on May 12, 2005. Spyware Bill 2005 (Austl.), *available at* http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?TABLE=BILLS&ID=1973.

weighed in on the legislative efforts of that country cautioning lawmakers about narrowly defining spyware.[47] The group would like legislation aimed at perpetrators of spyware to focus on the functionality of the software and "not the circumstances of it's [sic] installation on any particular computer."[48]

Canada has not passed any spyware-specific legislation but the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") outlines some Canadian laws that are relevant to spyware. They are similar to the FTC Act's prohibition of unfair and deceptive practices.[49]

The Netherlands was making preliminary plans for an anti-spyware bill in 2004 because the cost of dealing with spyware was becoming as high as the cost of viruses and spam.[50] A Dutch organization called Safe Internet Foundation ("SIF") has reported that 40% of consumer reports in 2003 were related to spyware.[51] However, there appears to have been no progress with spyware legislation in the Dutch Parliament. The European Union's approach to spyware will likely control how the Dutch handle the issue in the absence of more specific legislation in that member nation.[52]

Though the European Court of Justice has not issued a spyware directive this year, the European Union has joined with the United

---

[47] "EFA was established in 1994, is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties." Electronic Frontiers Australia, *Submission to Australia's Department of Communications, Information Technology and the Arts Public Consultation on Spyware,* (June 29, 2005), http://www.efa.org.au/Publish/efasubm-dcita-spyware-2005.html.

[48] The group also does not want the spyware definition to be broadened to include programs that use bandwidth and resources preferring those programs to be called malware. Australia has a privacy statute in place and EFA is as concerned about spyware with criminal uses such as theft from bank accounts as it is about spyware that spies for no apparent useful reason because it is an invasion of privacy. *Id.*

[49] CIPPIC, *Spyware FAQ*, http://www.cippic.ca/en/faqs-resources/spyware/ (last visited Feb. 13, 2006).

[50] Joe Figueiredo, *Dutch Parliament to Go After Autodialers, Spyware*, DMEUROPE.COM, June 7, 2004, http://www.dmeurope.com/default.asp?ArticleID=2247.

[51] *Id.*

[52] European Union Member States, http://europa.eu.int/abc/governments/index_en.htm (last visited Feb. 13, 2006).

States to implement the Declaration on Enhancing Transatlantic Economic Integration and Growth. One of the objectives listed in the Declaration is to "cooperate to tackle spam through joint enforcement initiatives, and explore ways to fight against illegal 'spyware' and 'malware.'"[53]

The legislative bodies of other countries may not be facing the pressures that the U.S. Congress faces to pass spyware-specific legislation or may simply be incapable of reacting to the problem as quickly as Congress has. It may be just as likely though that the EU and other countries are relying on their existing privacy protection and unfair trade practice law to deter the bad actors of the spyware world. The United States does not have the same kinds of privacy laws on the books as other countries and hence, it is approaching the spyware problem more directly.[54]

D. FEDERAL LITIGATION

The year 2005 saw many more enforcement actions against spyware in the federal courts. The FTC stepped up prosecutions of those who employed unfair and deceptive practices in distributing spyware to unsuspecting consumers. Consumer groups filed class

---

[53] Press Release, The White House, The United States and the European Union Initiative to Enhance Transatlantic Economic Integration and Growth (June 20, 2005), http://www.whitehouse.gov/news/releases/2005/06/20050620-17.html.

[54] European Union Directive 95/46/EC (Council Directive 95/46; 1995 O.J. (L 281) (EC)) governs privacy and regulates how personal data may be "collected, processed, used, and transferred." The law can be a major factor in U.S. companies' decisions to transfer data or to maintain data processing centers within the EU to avoid compliance problems. Rebecca S. Eisner, *Ignorance Isn't Bliss: What You Need to Know About EU Data Privacy Law*, CIO MAGAZINE, Mar. 1, 2002, *available at* http://www.cio.com/research/legal/edit/030102_eu.html.

While the governing bodies of the EU have broad power to make laws that become the law of the land for each member nation, often member states have to pass laws in their nations to enact EU directives. The EU is a relatively young organization whose roles and powers of enforcement have slowly evolved and become stronger over its approximate 60 year history. Member nations have only in the last decade started to take seriously the orders of the European Court of Justice now that fines are being assessed on member nations to enforce EU laws. *See* Steven Mulvey, *A Breakdown in EU Discipline?*, BBCNEWS.COM, July 14, 2005, http://news.bbc.co.uk/go/pr/fr/-/1/hi/world/europe/4680747.stm. While the EU's position on spyware is certainly important, member nations may need to take action themselves similar to how the individual states got the ball rolling in the U.S. See http://www.europa.eu for more information on the government of the European Union and the challenges it faces.

action lawsuits on behalf of spyware victims. Additionally, some 2004 cases were resolved and companies and consumers were given an idea of the kinds of legal theories that may or may not work in attacking spyware.

The FTC has filed a complaint in the U.S. District Court for the Central District of California in Los Angeles against several defendants, including Enternet Media, Inc. and Networld One, accusing them of distributing spyware that installs secretly and performs activities such as displaying pop-up ads; the FTC seeks 1) to bar the luring practices employed by the defendants, such as bundling spyware with free music and ringtone downloads, and 2) the forfeiture by defendants of any gains from their illegal activity.[55]

The complaint is a fine example of how consumers can make a difference. Individuals' reports of spyware attacks led to the FTC investigation of these defendants. The technology community sees this as a significant crackdown as well. Mona Spivack of the FTC's Bureau of Consumer Protection says the complaint alleges that tracking users' online activity violates their privacy.[56] Enternet Media Inc., Conspy & Co. Inc. and Networld One were all accused in this complaint.[57] Richard Stiennon of the Colorado anti-spyware firm Webroot, said that the EliteBar spyware program, thought to be created by Enternet Media, Inc., is third on the company's top-ten list of spyware programs.[58]

Other types of litigation arose from the anti-spyware industry. Companies sought declaratory judgments that would allow them to notify its users that certain adware presents a risk. For example, Symantec has filed a complaint in federal district court against Hotbar.com, Inc. after receiving a cease-and-desist letter from Hotbar telling Symantec to stop classifying Hotbar's product as spyware.[59] The FTC also settled two suits with anti-spyware companies that had

---

[55] Federal Trade Commission, *FTC Shuts Down Spyware Operation*, Nov. 10, 2005, http://www.ftc.gov/opa/2005/11/enternet.htm.

[56] Ryan Naraine, *FTC Shuts Down BlogSpot Spyware Ring*, EWEEK, Nov. 10, 2005, http://www.eweek.com/article2/0,1895,1885290,00.asp.

[57] *Id.*

[58] *Id.*

[59] Ryan Naraine, *Symantec Strikes Back at 'Adware' Vendor*, EWEEK, June 8, 2005, http://www.eweek.com/article2/0,1895,1825613,00.asp.

scanned users' machines and claimed to have found spyware where none existed.[60] The companies then sold their anti-spyware product to the users.[61] One of the defendants, MakTheater, Inc., is barred from future sales of anti-spyware products and services as a condition of the settlement.[62]

Sotelo v. DirectRevenue is a suit in which the plaintiff accused several defendants of willfully disregarding users' rights to use their computers as they please and damaging users' computers by installing spyware bundled with other legitimate software products.[63] The defendants removed this case from Illinois state court to federal district court and filed motions to dismiss the claims. Plaintiff sued DR Holdings, the parent company of DirectRevenue, LLC, but the court held that it did not have jurisdiction over the holding company. Plaintiff's claim of unjust enrichment against the remaining defendants was dismissed but the district court denied the remaining defendants' motions to dismiss other claims.[64] Further action in the suit is pending.

In a 2004, suit filed by 1-800 Contacts against WhenU.com, 1-800 Contacts claimed that WhenU.com violated 1-800 Contacts' copyright of their website by covering the site with pop-up advertisements; the court did not find a copyright violation but did grant an injunction of WhenU.com's practices finding that WhenU.com may have violated 1-800 Contact's trademark rights by causing source and/or initial interest confusion when it displayed competitor's ads to users of 1-800Contacts.com.[65] In 2005, the Second Circuit reversed the

---

[60] *Bogus Anti-Spyware*, *supra* note 5.

[61] *Id.* "'Scans' Detected Spyware That Wasn't There; Spyware Removal Software Claims Were False[;] Settlements Require Defendants to Give Up Nearly $2 Million in Ill-Gotten Gains."

[62] *Id.*

[63] Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219 (D. Ill. 2005); Eric L. Howes, *Lawsuit Filed against Direct Revenue*, Apr. 6, 2005, http://netrn.net/spywareblog/archives/2005/04/06/lawsuit-filed-against-direct-revenue/.

[64] *Sotelo*, 384 F. Supp. 2d at 1236.

[65] 1-800 Contacts, Inc. v. WhenU.com, 309 F. Supp. 2d 467, 510 (S.D.N.Y. 2003). *See also* Matthew Bierlein & Gregory Smith, *Privacy Year in Review: Growing Problems with Spyware and Phishing, Judicial and Legislative Developments in Internet Governance, and the Impacts on Privacy*, 1 ISJLP 279, 293-94 (2005) (detailed discussion of the original case).

preliminary injunction and dismissed the trademark infringement claims.[66] The Court held that the district court erred in finding that WhenU.com "used" 1-800 Contacts' trademark and therefore, 1-800 Contacts had failed to prove an essential element of trademark infringement. Though the Supreme Court denied certiorari in November 2005, the Second Circuit's decision suggests that copyright and trademark infringement claims may not be the best tools for combating spyware.[67]

L.L. Bean and Claria settled their dispute that originated in 2004 after Claria sought a declaratory judgment stating that their pop-up ads were not infringing L.L. Bean's trademark.[68] The settlement provisions are confidential, but Claria agreed to alter its advertisement delivery and pay a certain amount to L.L. Bean if L.L. Bean dropped its claims against Claria and its customers.[69] The Ninth Circuit declined to decide whether Claria's pop-up advertisements were legal because the company was no longer engaging in the specific conduct that had sparked the suit.[70]

While businesses fought each other over the harms of spyware, consumers stood up for their rights against spyware companies as well. Two consumer class action suits were brought against 180Solutions, Inc. in U.S. district courts. In September 2005, a consumer class action was filed in Illinois on behalf of all U.S. residents who have had 180Solutions software installed on their computers.[71] Also, in October 2005, a further class action was filed in

---

[66] 1-800 Contacts, Inc. v. WhenU.com, Inc., 414 F.3d 400, 407 (2d Cir. 2005).

[67] 1-800 Contacts, Inc. v. WhenU.com, Inc., 126 S. Ct. 749 (2005).

[68] Out-Law.com, *Pop-up Ads Cases Settled By L.L. Bean*, Jan. 1, 2005, http://www.out-law.com/page-4677.

[69] *Id.*

[70] The appeal went forward in February 2005 even though the parties settled in summer 2004 following oral argument of the case. The issue before the court was whether the declaratory judgment action was moot after the settlement between the parties. The opinion refers to Claria as Gator, the name under which the company did business when the dispute began in 2001. The 9th Circuit decided that the case was moot. "Because the parties' settlement agreement has wholly eviscerated the dispute that prompted Gator to initiate this suit, Gator's request for declaratory relief no longer gives rise to a live case or controversy." Gator.com Corp. v. L.L. Bean, Inc., 398 F.3d 1125, 1131 (9th Cir. 2005).

[71] Wendy Davis, *180Solutions Hit with Lawsuit*, ONLINE MEDIA DAILY, Sept. 15, 2005, http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art

California by Consumer Advocates Rights Enforcement Society ("CARES").[72]

The increased action by the FTC is probably the most promising development to come out of 2005. The FTC's power to hold spyware vendors accountable will only grow with the passage of federal legislation that could take place in 2006. However, even without such legislation, the FTC may successfully deter the proliferation of spyware with its current arsenal of authority.

E. STATE LITIGATION

Although the most important developments took place in federal court, litigation also commenced in state courts under the new state spyware laws. For example, the Texas Attorney General and an individual in California brought suits in their respective state courts against Sony for secretly installing software on users' machines when they used Sony CDs.[73] The software slowed the performance of users' machines and is very difficult to remove. A New York case was settled in October after Attorney General Elliot Spitzer filed suit in April 2005 against Intermix, a Los Angeles company that had distributed spyware to New Yorker computer users, and Acez Software, which had bundled Intermix software with its product. The cases were brought "under traditional state 'deceptive practices' and 'false advertising' laws, contained in the New York General Business Law."[74]

_aid=34089. Complaint, Simios v. 180Solutions, Inc., No. 05C-5235, (N.D. Ill. E. Div. Sept. 13, 2005), *available at* http://www.sunbelt-software.com/ihs/alex/180class.pdf.

[72] Bronson & Associates, *Pending Class Action Lawsuits*, http://www.thelaw.bz/ClassActionLawsuits.htm, (last visited Feb. 13, 2006); Notice of Removal, Consumer Advocates Rights Enforcement Society, Inc. v. 180Solutions, Inc., No. CV027141 (E.D. Cal. Dec. 14, 2005), *available at* http://www.sunbelt-software.com/ihs/alex/show_case_doc.pdf.

[73] "According to the Electronic Frontier Foundation (EFF), co-counsel in the California case, Sony BMG has caused damage by virtue of First4Internet XCP (XCP) and SunnComm MediaMax software that it included in more than 24 millon music CDs." Eric Sinrod, *Legal Woes Mount for Sony BMG Resulting From Its CD Software*, MODERN PRACTICE, Nov. 29, 2005, http://practice.findlaw.com/tooltalk-112905.html.

[74] Press Release, Office of NYS Attorney General Eliot Spitzer, Internet Exec Held Responsible for Adware, Spyware (Oct. 20, 2005), http://www.oag.state.ny.us/press/2005/oct/oct20a_05.html.

In 2004, WhenU.com challenged Utah's spyware statute and obtained an injunction against its enforcement.[75] That case is probably moot now that the law has been amended and basically rewritten. No additional documents were filed in the case in 2005. The future may see more challenges under existing state laws and new anti-spyware statutes. Additionally, other state laws, like Utah's Spyware Control Act, could face constitutional challenges. For example, an Alaska law considered to be much broader than other state spyware laws may be open to future court challenge on First Amendment and dormant commerce clause grounds, but such a case would likely be brought in federal court.[76]

F. CONCLUSION

There was a big increase in 2005 in the amount of proposed legislation and litigation initiated in the area of spyware. While this may lead to a decrease in fraud and privacy invasions perpetrated on consumers, perpetrators of illegal spyware installation and use will probably need to see more enforcement of existing and new law before they are dissuaded. There will likely be attempts by unscrupulous actors to defraud and intrude on other businesses and consumers before lawmakers get a complete grasp of the possible infringements of rights that are enabled by technology. Legislators have to be careful not to open windows where doors have been shut. While these solutions may not be very far off, Congress has a bit more work to do. With active privacy and technology watchdog groups in the mix, such a the Center for Democracy and Technology, at least Congress will have help in designing laws to protect consumers from new threats.

II. PHISHING AND SPOOFING

Phishing is a type of "e-mail fraud where the perpetrator sends out legitimate-looking e-mails that appear to come from well known and trustworthy web sites in an attempt to gather personal and financial information from the recipient."[77] Phishers believing that obtain

---

[75] GOLDMAN BLOG, *supra* note 42.

[76] Privacy Law Watch, *Tough Anti-Adware Alaska Law Signed By Governor, Banning Almost All Pop-Up Ads*, Sept. 2, 2005, http://subscript.bna.com/SAMPLES/pra.nsf/0/90b3be53ce72c8918525707000022ddc?OpenDocument.

[77] *Phishing – A Whatis.com Definition*, SEARCHSECURITY.COM, Oct. 17, 2005, http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci916037,00.html. This

information from their targets by scaring users into thinking one of their accounts, a PayPal account for example, has been closed or – worse – violated by an Internet con artist. Spoofing, in this context, involves fooling users by putting up a web site that purports to be that of a legitimate business for the purpose of collecting valuable information from an unsuspecting visitor. Phishers try to direct users to spoofed web sites as part of their schemes. However, it should be noted that spoofing can also refer to a legitimate technique for managing network traffic.[78]

The Anti-Phishing Working Group ("APWG") monitors phishing activity each month. Its December 2005 report is very revealing of phishers' behavior. The top 80% of phishing campaigns targeted only seven brands, 51% of sites use part of their target brand's name in the URL and the average length of time that a spoofed site stays operational is 5.3 days. This report only represents a synopsis of the phishing attacks that are reported to the Group but is nonetheless enlightening as to the scope of the problem. The Group received over 15,000 reports in December identifying over 7,000 unique phishing sites, a huge increase over the previous two months.[79] Additionally, the Group reported on a Websense Security Labs study that identified the United States as the reigning number one host of phishing websites with 34.67%.[80] The next closest countries were China and Korea each with close to 9% of phishing websites hosted in their countries.[81] The APWG's December report reveals a problem that continues to grow rapidly.[82]

---

author can attest to PayPal's frequent spoofing having just received an email with the subject "Your PayPal account has been violated!" containing links purporting to go to http://www.paypal.com but that actually direct users to http://www.chinesecommunity.us/albums/album01/temp.php.

[78] Webopedia, What is Spoof?, http://www.webopedia.com/TERM/S/spoof.html (last visited Feb. 13, 2006).

[79] The Anti-Phishing Working Group (APWG) is dedicated to combating phishers and the havoc they wreak on consumers. Anti-Phishing Working Group, *Phishing Activity Trends Report*, (Dec. 2005), http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf.

[80] *Id.*

[81] *Id.*

[82] *Id.*

Because of the potential for phishers to steal users' identities, consumers are at great risk when they fall for a phisher's scam. Besides the inconvenience of dealing with these bogus emails, computer users face an egregious form of trickery that seriously threatens their privacy rights. An even bigger concern is the endangerment of the Internet's power as a tool to unite and aid in business and personal communication. There are several options for going after perpetrators as phishing falls under a few different areas of regulation.[83] While no federal law was passed in 2005 specifically targeted phishing, California earned the distinction of being the first state to pass anti-phishing legislation.

A. FEDERAL LEGISLATION

Federal legislation regarding the practice of phishing may pass in early 2006. A version of The Anti-Phishing Act of 2005 was introduced in both the House and the Senate after the Anti-Phishing Act of 2004 failed to make it through Congress the previous year. The Act provides for penalties of fines and imprisonment for the criminal act of creating a web site or sending e-mails to trick a user into communicating with what target computer users believe to be a legitimate online business and revealing their personal information.[84]

Some progress was made in the direction of outlawing phishing practices when the House passed the Internet Spyware ("I-SPY") Prevention Act of 2005 on May 23, 2005; though the bill's focus is spyware, it includes in its appropriation to the Attorney General's office direction to use the funds to prosecute phishing activities as well.[85] The bill proposes the authorization to appropriate $10,000,000 each year from 2006 through 2009 for prosecutions by the Attorney

---

[83] *See* Bierlein & Smith, *supra* note 65, at 300-301 (discussion of phishing activities falling under laws governing identity theft, wiretapping, bank fraud, computer fraud and abuse, and the Federal Trade Commission Act).

[84] S. 472, 109th Cong. (1st Sess. 2005). H.B. 1099, 109th Cong. (1st Sess. 2005). H.B. 1099 was referred to the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security on May 10, 2005. S. 472 was submitted to the Senate Committee on the Judiciary on February 28, 2005. Both bills are significantly similar to the 2004 version of the Anti-Phishing Act. *See* Bierlein & Smith, *supra* note 65, at 310 (detailed discussion of the Anti-Phishing Act of 2004).

[85] I-SPY, H.R. 744, 109th Cong. (1st Sess. 2005). The bill was referred to the Senate Committee on the Judiciary on May 24, 2005.

General "to discourage the use of spyware and the practices commonly called phishing and pharming."[86] The bill does not define the methods of phishing too narrowly but instead criminalizes the intentional acts of obtainment or transmission of personal information or the impairment of security programs on users' computers "with the intent to defraud or injure a person or cause damage to a protected computer."[87] Given that the Senate has moved forward to combat spyware by approving the SPY BLOCK Act instead of the I-SPY Act, this is probably not the phishing solution consumers need. Enforcement actions against phishers may have to arise under the FTC's existing laws to prosecute fraud and unfair or deceptive practices or under the future authority of laws that specifically target phishing.

B. STATE LEGISLATION

California is the first state to have passed an anti-phishing law. On October 3, 2005 the Anti-Phishing Act of 2005 was signed into California law. The Act "makes it unlawful for any person, through the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the approval or authority of the business."[88] Victims can seek the greater of actual damages or $500,000 per violation, and fines of up to $2,500 per violation may be assessed as well.[89]

---

[86] *Id.* "Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect." Webopedia, What is Pharming?, http://www.webopedia.com/TERM/p/pharming.html (last visited Feb. 13, 2006).

[87] H.R. 744, 109th Cong. § 1030A(b)(1) (1st Sess 2005).

[88] Gregg Keizer, *California Enacts Tough Anti-phishing Law*, TECHWEB NEWS, Oct. 3, 2005, http://banktech.com/showArticle.jhtml?articleID=171202671.

[89] *Id.*

C. INTERNATIONAL LEGISLATION

Though India has not passed any official legislation to combat phishing, the Delhi high court has declared phishing illegal, allowing recovery of damages and injunction.[90] The Court gave an example of phishing, stating that "typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details."[91] The plaintiff in this case was National Association of Software and Service Companies, a group with 850 member organizations, 150 of which are global companies.[92] This was a breakthrough case because it solidly establishes that damages are available for intellectual property violations in India.[93] As U.S. companies continue to expand into India, this move helps to reassure them that Internet crimes and attacks on their businesses will not be ignored.

D. FEDERAL LITIGATION

Microsoft filed suit in federal court against 117 defendants for phishing attacks that targeted their Hotmail customers from October 2004 to March 2005.[94] The goal of the suits was to discover links between phishers worldwide so as to take out the larger forces in this area. Trademark law forms the basis of the legal claims as the phishers are appropriating Microsoft trademarks in e-mails and on fake web sites. The theory could have greater success in prosecuting phishers than spyware purveyors because there is a clear use of trademarked symbols and logos in phishing activities. Aaron Kornblum, Microsoft's Internet safety enforcement attorney, said, "Today, we're filing more phishing lawsuits in one day than we have

---

[90] Diljeet Titus and Sumit Roy, *Phishing on the Net*, ASIALAW, June 2005, http://www.asialaw.com/default.asp?page=14&ISS=16853&SID=518004.

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] Grant Gross, *Microsoft Files 117 Phishing Lawsuits*, PCWORLD, Mar. 31, 2005, *available at* http://www.pcworld.com/news/article/0,aid,120258,00.asp.

filed spam lawsuits in the prior year and a half."[95] This indicates a shift in focus in the litigation arena away from spam and toward the more serious phishing activities. This is similar to the lawmakers' shift, albeit a slow-moving one, in the focus of legislation away from yesterday's spam and viruses to today's phishing menace.

E. CONCLUSION

Phishing is a very dangerous practice to consumers. The Anti-Phishing Act will hopefully pass in 2006. The existence of a patchwork of non-uniform state phishing laws would not have the same impact on legitimate businesses as having multiple state spyware laws. There is no risk to a legitimate business activity because nothing resembling a legitimate activity is being attempted by phishers; there is an obvious primary intent to defraud and harm consumers directly. Having a federal standard will be useful for the states, which probably do not have much of an interest in tailoring their laws to combat phishing and every new malicious technology that comes along. A federal standard could also help in dealing with international threats from phishing. As the phishing problem grows, so must the effort to combat it. The year 2005 showed an increased awareness of the problem, and hopefully, a readiness to take it on.

---

[95] Andrew Noyes, *Don't be 'Phooled,' Anti-Phishing Advocates Warn Consumers*, WASH. INTERNET DAILY, Apr. 1, 2005.