Richmond Journal of Law and Technology

Volume 13 | Issue 1 Article 3

2006

Bigger Phish To Fry: Californias Anti- Phishing Statute And Its Potential Imposition Of Secondary Liability On Internet Service Providers

Camille Calman

BIGGER PHISH TO FRY: CALIFORNIA'S ANTI-PHISHING STATUTE AND ITS POTENTIAL IMPOSITION OF SECONDARY LIABILITY ON INTERNET SERVICE PROVIDERS

Camille Calman *

[1] The incidence of phishing, a form of internet fraud, has increased dramatically since 2003.[1] Identity thieves searching for vulnerabilities in internet security have realized that customers are the weak link.[2] Using mass e-mailings and websites purporting to be those of well-known and trusted corporations, "phishers" trick customers into revealing personal and financial information.[3] Once in the hands of phishers, that

*Associate, Debevoise & Plimpton LLP; J.D., Columbia Law School, 2006. I would like to thank Professor Hillel Parness for teaching the seminar that led me to write this article.

[1] *See* ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT (June 2006), *available at* http://www.antiphishing.org/reports/apwg_report_june_2006.pdf [hereinafter APWG June 2006 Report] (showing a record high number of reported phishing attacks, 28,571, in June 2006); DEP'T OF JUSTICE, SPECIAL REPORT ON "PHISHING" (2004), *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf [hereinafter DOJ Report] (describing rise in phishing from 2003 to late 2004); Ravi Puri, *Gone Phishing: Protecting Online Identity*, OR. ST. B. BULL., Oct. 2004, at 37 (describing a recent rise in phishing). One study shows that one in four Americans receive a phishing attack monthly, and that 70% of those users think the e-mail comes from a legitimate company. AM. ONLINE & NAT'L CYBER SEC. ALLIANCE, AOL/NCSA ONLINE SAFETY STUDY 3 (Dec. 2005) *available at* http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

[2] *See* Clare Francis, *Alert Over Risks of E-Banking*, SUNDAY TIMES (London), Aug. 22, 2004, at Features 5 (quoting an information technology professional as saying, "The banks' systems are pretty secure, which is why fraudsters are targeting customers – they are the weakest link").

[3] Jefferson Lankford, *The Phishing Line*, ARIZ. ATT'Y, May 2005, at 14. The Department of Justice defines phishing as "criminals' creation and use of e-mails and websites, designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies, in order to deceive internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords." DOJ Report, *supra* note 1, at 1.

information can be used to clean out bank accounts, go on credit card spending sprees, defraud third parties,[4] or to open accounts for credit cards, loans, or mortgages.[5] Information can also be sold to other thieves.[6] Individual customers lost an estimated $929 million to phishing scams from May 2004 to May 2005,[7] and they are not the only victims. Financial institutions and other businesses lose an estimated $2 billion a year to phishing scams.[8]

[2] Legislatures have passed new laws in response to media reports of phishing. In January 2005, Virginia added phishing to its Computer Crimes Act, categorizing the use of a computer to obtain personal information "through the use of material artifice, trickery or deception" as a Class 6 felony punishable by prison sentences of up to five years and fines of up to $2,500.[9] New Mexico enacted a similar statute in March of

[4] For instance, phishers often hijack the accounts of eBay users in order to defraud other eBay users by listing auctions and accepting payment for items that do not exist. *See* Ian Austen, *On eBay, E-Mail Phishers Find a Well-Stocked Pond*, N.Y. TIMES, Mar. 7, 2005, at C2 (profiling coin dealer whose eBay account was hijacked and used to sell $780,000 worth of fraudulent items); Amardeep Bassey, *Netted: Trio Jailed for eBay "Phishing" Scam*, SUNDAY MERCURY (Birmingham, U.K.), Nov. 13, 2005 at 13 (describing eBay fraud scheme that brought in £500,000).

[5] *See* Larry Williams, *Restoring Their Credit, Reclaiming Their Lives: Crime: Victims of Identity Theft Find Limited Resources in the Struggle to Clear Their Name*s, BALT. SUN, Feb. 27, 2005, at 1C.

[6] *See* Bill Toland, *Watch That Hook: With Just a Couple Clicks, Internet Users Can Become Part of a "Phishing" Harvest*, PITTSBURGH POST-GAZETTE, Dec. 12, 2005, at Science A1.

[7] Press Release, Gartner, Inc., Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce (June 23, 2005), *available at* http://www.gartner.com/press_releases/asset_129754_11.html. (stating that survey participants indicated that financial institutions reimbursed them for most of those losses).

[8] Paul L. Kerstein, *Talk Back: How Can We Stop Phishing and Pharming Scams?*, CSO, July 19, 2005, *available at* http://www.csoonline.com/talkback/071905.html. Statistics relating to phishing loss may not be entirely reliable; it is not clear, for example whether some of the losses are being double-counted, attributed first to the consumers who suffer them, and then to the banks which make good on the consumers' losses.

[9] VA. CODE ANN. § 18.2-152.5:1 (2005); *see also* Larry Greenemeier, *States Tell Phishers to Cut Bait or Else: Virginia and New Mexico Set to Enforce New Laws That Categorize Phishing as a Felony*, INFO. WK., Apr. 13, 2005, *available at* http://www.informationweek.com/showArticle.jhtml?articleID=160702186; *AOL Sues Over IdentityThefts, Uses New Law*, REUTERS, Feb. 27, 2006, *available at*

2005,[10] as did New York in June of 2006.[11] Bills like these have been considered in many other states, including Pennsylvania[12] and Florida.[13] The state of Washington has gone even further by criminalizing attempted phishing. Both the sending of "spoof" e-mails and the setting up of fraudulent websites are considered criminal activities, even if no consumer is defrauded by either action.[14] At the federal level, U.S. Senator Patrick Leahy has introduced a bill, the Anti-Phishing Act of 2005, which is similar to the Washington state bill in punishing any attempt at phishing even if no identity theft or other consumer damages result.[15]

[3] Bills that define phishing and attempted phishing as crimes are good public relations moves for legislators, since they give an impression of government taking active steps to wipe out a dangerous new crime. But such legislation ignores the fact that phishing and attempted phishing are already crimes. Fraud and identity theft have never been legal activity; the only factor that makes phishing "new" is the particular electronic method used to con the target out of his or her personal information.[16] By

---

http://today.reuters.com/news/articlebusiness.aspx?type=telecomm&storyID=nN27331008&from=business.

[10] S.B. 720, 2005 Leg., Reg. Sess. (N.M. 2005), N.M. STAT. ANN. § 30-16-24.1 (West 2005).

[11] Assemb. 8025, 2005 Assemb., Reg. Session (N.Y. 2005); *see also* Press Release, Governor George E. Pataki, Governor Signs Important Legislation to Protect New Yorkers Against Identity Theft (June 9, 2006), *available at* http://www.ny.gov/governor/press/06/0609061.html.

[12] H.B. 2292, Gen. Assem. 2005, Reg. Sess. 2005–2006 (Pa. 2005).

[13] H.B. 7157, 2006 Leg., Reg. Sess. (Fla. 2006).

[14] H.B. 1888, 2005–2006 Leg. Reg. Sess. (Wash. 2005), WASH. REV. CODE § 19.190.010 (2005); *see also* Eric Chabrow, *Washington State Enacts Anti-Spyware and Anti-Phishing Legislation*, GOV'T ENTERPRISE, May 19, 2005, *available at* http://www.governmententerprise.com/news/163105506.

[15] S. 472, 109th Cong. (2005); *see also* Press Release, Senator Patrick Leahy, New Leahy Bill Targets Internet "PHISHING" and "PHARMING" That Steal Billions of Dollars Annually from Customers (Feb. 28, 2005), *available at* http://leahy.senate.gov/press/200503/030105.html. The bill is virtually identical to the Anti-Phishing Act of 2004, which was still in committee when the previous Congress adjourned. Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation Versus Technology*, 2005 DUKE L. & TECH. REV. 0006, at ¶5 (Mar. 14, 2005), *available at* http://www.law.duke.edu/journals/dltr/articles/2005dltr0006.html.

[16] Phishers may also be violating criminal provisions of the CAN SPAM Act, particularly 18 U.S.C. § 1037, which criminalizes falsifying e-mail account information, falsifying

declaring that phishing is now a crime, legislators do little more than state the obvious.[17] Such measures should not reassure consumers, since phishers often operate offshore and are not available for criminal prosecutions in state courts.[18] Criminal penalties will have little deterrent effect if they cannot be enforced.[19] As long as phishing remains a low-cost, low-risk crime, criminals will continue to phish.

[4] California has taken a more interesting approach in its anti-phishing statute, which was signed into law in September 2005.[20] The bill provides for civil, rather than criminal, penalties against phishers.[21] Individuals who are victims of identity theft have a cause of action, but only against those who have "directly violated" the statute—the phishers themselves.[22] However there is no such caveat in the section of the statute allowing suits by an entity which is "engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark."[23] The existence of the word "direct" in the paragraph pertaining to individuals, and its absence in the paragraph pertaining to entities, suggests that the entities can sue indirect violators—for instance, the internet service providers (ISPs) who provide phishers with e-mail access and web space.[24] These are both easier for plaintiffs to track down and deeper of

---

header information, and relaying spam. 18 U.S.C. § 1037(a) (2005). Violators can face prison terms, fines, and forfeiture of proceeds from the crime(s). *Id.* at § 1037(b).

[17] *See* Gene S. Koprowski, *Tough State Laws Won't Stop "Phishing" Scams, Experts Say*, TECHNEWSWORLD, Oct. 29, 2005, http://www.technewsworld.com/story/46889.html [hereinafter Koprowski, *Tough Laws*] (quoting Jim Harper, Director of Information Policy Studies at the Cato Institute: "Politicians who claim to protect consumers in this environment either don't know that they are lying, or are deeply cynical").

[18] *Id.* (quoting a computer security expert, Naftali Bennett, as saying that 70% of phishers are overseas, and adding: "[I]t's almost impossible to track down and prosecute the fraudsters . . . Phishers are growing more sophisticated in masking their identities and locations. They're taking over PCs – as zombies – and hiding very effectively").

[19] *Id.* (quoting Bennett as saying, "It's still incredibly easy to do, the rewards are very high, and the chances of actually getting caught are still very low. Until one or more of these factors change, I don't expect phishing attacks to decline").

[20] CAL. BUS. & PROF. CODE § 22948–22948.3 (West Supp. 2006).

[21] *Id.*

[22] *Id.* § 22948.3(a)(2).

[23] *Id.* § 22948.3(a)(1).

[24] *See id.*; *see also* Gene J. Koprowski, *Critics Doubt Effectiveness of California Anti-Phishing Law*, EWEEK.COM, Oct. 5, 2005,

pocket. Yet, nothing in the statute's legislative history suggests that legislators intended to create such liability.[25] ISPs may be able to avoid prosecution under the safe harbor provided by the Communications Decency Act (CDA).[26] But, in order to do so, the ISPs may need to take affirmative steps to investigate and act on complaints about phishers.[27]

[5] This paper explores whether California's statute will lead to imposition of secondary liability for phishing, and whether this would have the effect of decreasing phishing. Part I explains how phishers operate and why criminal law has been largely ineffective in deterring phishers. Part II studies the California anti-phishing statute and its legislative history, as well as judicial precedents that suggest secondary liability may be available in California. Finally, part III discusses whether imposing secondary liability on ISPs is likely to be a practical tool in the war against phishing.

I: A BRIEF HISTORY OF PHISHING

[6] The term "phishing" has been in use at least since 1996, when computer hackers used it to describe tricking America Online (AOL) users out of their passwords so that their AOL accounts could be used.[28] Victims of the scam were known as "phishies."[29] AOL fought back using both technical and informational means: it began quickly terminating

---

http://www.eweek.com/article2/0,1895,1867673,00.asp [hereinafter Koprowski, *Critics*] (quoting attorney Dan Venglarik: "[W]hile the law is likely to be ineffective, and while it's doubtful that anyone will ever collect on a judgment against a phisher, there is real potential liability for ISPs and Web site hosting services if they don't start investigating and acting on complaints that their resources are being used for phishing").

[25] *See infra* note 77 and accompanying text.

[26] 47 U.S.C. § 230 (2000). California may offer a more hospitable climate than most states for plaintiffs trying to impose liability on ISPs. *See infra* notes 89–103.

[27] *See* Koprowski, *Critics*, *supra* note 24.

[28] WIKIPEDIA, *Phishing*, at http://en.wikipedia.org/wiki/Phishing (last visited Sept. 16, 2006). (stating that the "ph" is said to derive from the hacker term "phone phreaking," used to describe a technique for fraudulently obtaining free long distance calls from the telephone company). The AOL scam was mentioned in a 1997 newspaper article, the first media reference to "phishing" that is not a pun on the name of the band Phish. Ed Stansel, *Don't Get Caught by Online 'Phishers' Angling for Account Information*, FLA. TIMES-UNION (Jacksonville, Fla.), Mar. 16, 1997, at G-3.

[29] *Id.*

accounts involved with phishing and it alerted users, adding a line at the bottom of all instant messages that read, "No one working at AOL will ask for your password or billing information."[30] Once AOL began offering unlimited online access for a flat rate rather than billing by the hour, phishers had less incentive to steal other users' passwords.

[7] But the damage was done. Thieves had learned that the easiest way to obtain private information was simply to ask for it, preferably while pretending to be someone else—a pretense made far easier by the internet's anonymity.[31] As more Americans began to do their banking and conduct other transactions online,[32] consumers became accustomed to dealing with banks and e-commerce sites by sending and receiving e-mails.[33] An e-mail asking a user to confirm his or her information now seems to many users to be part of the routine course of internet business.

[8] The typical phishing incident involves two steps.[34] First, the phisher obtains web space from a service provider and sets up a website designed to mimic or "spoof" that of a financial institution, internet service provider, or e-commerce site.[35] The most popular targets include AOL, Bank of America, Citibank, Washington Mutual, eBay, and PayPal.[36]

---

[30] *Id.*

[31] *See* Michael Rogers, *Let's See Some ID, Please: The End of Anonymity on the Internet*, MSNBC.com, Dec. 13, 2005, http://www.msnbc.msn.com/ID/10441443 ("[A]lthough anonymity has been part of Internet culture since the first browser, it's also a major obstacle to making the Web a safe place to conduct business.").

[32] Forty-three percent of American internet users now bank online. *See* Susannah Fox and Jean Beier, *Online Banking 2006: Surfing to the Bank* (June 14, 2006), http://www.pewinternet.org/pdfs/PIP_Online_Banking_2006.pdf.

[33] Indeed, some e-commerce sites offer only online customer service rather than telephone support. For instance, eBay offers telephone support only to the high-volume sellers known as "Powersellers" and to sellers who pay monthly fees to operate an "eBay Store." All other users can receive help only online or via e-mail. Laura Rohde, *eBay to Boost Support, Cut Fees*, PC WORLD, Feb. 7, 2005, *available at* http://www.pcworld.com/news/article/0,aid,119594,00.asp. Because users expect to hear from eBay only via e-mail, they are more receptive to e-mails from phishers than they might be otherwise.

[34] Puri, *supra* note 1, at 37.

[35] *Id.*

[36] Lankford, *supra* note 3, at 14; *see also* Press Release, Informatica Corp., Toronto Security Experts Release Ready to Use Anti-Phishing Security Policy (Nov. 22, 2004), *available at* http://www.canadait.com/cfm/index.cfm?It=106&Id=21120&Se=0&Lo=443

Government agencies such as the Internal Revenue Service[37] or the Federal Deposit Insurance Corp (FDIC)[38] may also be "spoofed." Phishers duplicate the look of the targeted site as exactly as possible, using similar fonts and graphics[39] as well as trademarked names and logos.[40] Next, the phisher sends out a mass e-mailing, with the same logos and graphics and a false "from" address.[41] Recipients are warned that there is an urgent need to update their information with the alleged sender, either because the sender has detected fraudulent use of their account, or because their account faces suspension unless they provide information.[42] Some recipients—from five to fifteen percent of them, according to some studies[43]—will be frightened enough by the warnings that they will click

[hereinafter Informatica Press Release] ("[T]he vast majority of phishers use one of 44 major brands to gain the trust of their victims."). The most popular brand among phishers is PayPal. One study found that 54.3% of phishing e-mails were attempts to steal information from PayPal customers. *Over 75% of All Phishing Emails Target PayPal and EBay Users*, INFOZINE, Aug. 5, 2006, *available at* http://www.infozine.com/news/stories/op/storiesView/sid/16858/. eBay ranked second, with 20.9%. *Id.*

[37] *IRS Issues Advisory on "Phishing" Scams*, PORTSMOUTH HERALD, July 31, 2006, *available at* http://www.seacoastonline.com/news/07312006/nhnews-ph-por-irs.scams.html.

[38] FDIC, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT 9 (2004), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf [hereinafter FDIC Report] (describing six separate phishing attacks against FDIC in year before report was written).

[39] Tracy Baker, *Ignore the Bait: Don't Get Hooked by Phishing Scams*, 16 PLUGGED IN 2, 54 (Feb. 2005).

[40] Thomas J. Smedinghoff, *Phishing: The Legal Challenges for Business*, BANKING & FIN. SERVICES POL'Y REP. 1, Apr. 2005; *see also* Jennifer Lynch, Note, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Fishing Attacks*, 20 BERKELEY TECH. L.J. 259, 259 (2005).

[41] Smedinghoff, *supra* note 40.

[42] Lynch, *supra* note 40, at 259.

[43] One article estimates that 70% of internet users have received phishing emails and that about 15% of those have been duped. Smedinghoff, *supra* note 40, at 2. The Anti-Phishing Working Group, an industry association of corporations and law enforcement organizations concerned about phishing, estimates that the response rate for phishing e-mails is about 5%. ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT (Jan. 2005), *available at* http://www.antiphishing.org/APWG_Phishing_Activity_Report-January2005.pdf [hereinafter APWG Jan. 2005 Report]. Ordinary spam has only a .01% response rate. Laura Sullivan, *FBI on Trail of E-Mail Fraud*, BALT. SUN, Feb. 13, 2004, at 2A.

on the enclosed hyperlink, go to the fake website, and submit their personal information.[44]

[9] Early phishing e-mails were often easily detectible, at least by savvy users. They were frequently laden with typographical, grammatical, and spelling errors.[45] The hyperlinks were often entirely numerical,[46] indicating to the knowledgeable user that the page to which they linked was not an actual AOL or Citibank web page. Also, the e-mails were often sent indiscriminately, reaching many users who did no business with the bank or website in question.

[10] But phishers have grown more sophisticated. Today's phishing e-mails tend to be grammatically correct,[47] though their titles may include misspellings to evade spam-detection filters.[48] Many phishers now target users whom they know to be customers of the entity they are impersonating, a technique known as "spear-phishing."[49] Further, phishers have developed techniques for masking the actual URL of their fraudulent site and allowing the URL of the real company's site to appear in its place on the user's web browser.[50]

---

[44] Information requested by phishers includes account numbers, passwords, credit card numbers, Social Security numbers, and dates of birth. Lankford, *supra* note 3, at 14.
[45] *See* Joan Collier, *Sales, Service, Security: The Big Three of Internet Marketing*, FLA. UNDERWRITERS, Apr. 2005, at 19.
[46] Lankford, *supra* note 3, at 14.
[47] Informatica Press Release, *supra* note 36. One reason for the upgrading of grammar and spelling is that phishers can now download free do-it-yourself phishing kits, with pre-written e-mails as well as the graphics, web code, and spamming software necessary to launch a phishing attack. John Leyden, *DIY Phishing Kits Hit the Net*, THE REGISTER (U.K.), Aug. 19, 2004, at http://www.theregister.co.uk/2004/08/19/diy_phishing/.
[48] Lankford, *supra* note 3, at 14.
[49] Timothy L. O'Brien, *For a New Breed of Hackers, This Time It's Personal*, N.Y. TIMES, Dec. 4, 2005, § 3, Col. 2, pg. 1 (discussing how some spear-phishing is alarmingly specific, mimicking messages from the user's employer or university credit union).
[50] *See* Lynch, *supra* note 40, at 269 (describing a technique that "replaces the 'Address' bar at the top of the victim's browser with an appropriately-designed working fake . . . [which] remains installed even after the consumer leaves the fraudulent site and allows the phisher to track the consumer's Internet movement as well as all of the information the victim sends and receives"). Even more alarming is a technique called "pharming," which is beyond the scope of this paper, but which redirects users, without their knowledge or consent, from real websites whose URLs they have typed to identical-

[11] While it might be tempting to blame the unsophisticated victims who have voluntarily given their information to thieves,[51] phishing victims are more sympathetic than many other victims of online fraud. Victims of the notorious "Nigerian scam" were motivated by the prospect of getting rich quickly with little effort.[52] Victims of internet auction scams are enticed by the fantasy of getting a plasma TV or other big-ticket items for a bargain-basement price.[53] But phishing victims are motivated by fear and by trust of the institutions with which they do business.[54] Phishing e-mails, ironically, often take advantage of that faith by describing the information requested as part of new security measures being implemented by the trusted website.[55]

[12] Although slippery, phishers are not completely uncatchable. Occasionally they are located and criminally prosecuted. Recently, a Florida man has been indicted in Pennsylvania for a phishing scam that mimicked a Hurrican Katrina relief website.[56] In 2004, Zachary Keith Hill plead guilty in a Texas federal court to crimes related to phishing activity and was sentenced to 46 months imprisonment.[57] In England, 20-year-old

looking but fraudulent sites. *See generally* Michelle Delio, *Pharming Out-Scams Phishing*, WIRED NEWS, Mar. 14, 2005, http://www.wired.com/news/infostructure/0,1377,66853,00.html.

[51] Even the U.S. House of Representatives cannot resist the temptation to scold the victims. *See* H.R. REP. NO. 108-698, at 5 (2004), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:hr698.108.pdf ("[M]ost phishing scams require the willing participation of the recipient to either visit a website or reply to an email and give out personal information. As in earlier forms of fraud using the mail or telephones, common sense and a healthy level of suspicion go a long way toward not becoming a victim of phishing.")

[52] *See* Marisa Schultz, *Bet on It: Online Lotto Scams Soar; Feds Warn Against Sweepstakes, Nigerian Letter Schemes That Are Too Good to Be True*, DETROIT NEWS, Jan. 11, 2005, at 1A; Barbra Mikkelson, *Nigerian Scam*, SNOPES.COM, http://www.snopes.com/crime/fraud/nigeria.asp (last updated Sept. 6, 2003).

[53] *See* Joe Morgan, *Bid Goodbye to Your Money*, THE TIMES (LONDON), Feb. 19, 2005, at Money 12.

[54] *See* Smedinghoff, *supra* note 40, at 2.

[55] *Id*.

[56] John Leyden, *Florida Man Indicted over Katrina Phishing Scam* , REGISTER (U.K.), Aug. 18, 2006, http://www.theregister.com/2006/08/18/hurricane_k_phishing_scam/.

[57] Plea Agreement at 1, United States v. Hill, Criminal No. H-04-, (S.D. Tex. 2003), 2003 WL 23338642 (S.S. Tex. 2003); Puri, *supra* note 1, at 39 (noting 46-month sentence).

American fugitive, Douglas Havard, was sentenced in 2005 to six years in a British prison for his part in a multi-million dollar international phishing scheme.[58] The U.S. Department of Justice has successfully prosecuted several other defendants in U.S. courts.[59]

[13] In general, though, criminal law does a poor job of deterring phishing,[60] largely because phishers are so hard to find.[61] As of January 2005, the average phishing site was active for only 5.8 days,[62] by June 2006 that time had dropped to 4.8 days.[63] Even if the victims notice and report the identity theft within that time, law enforcement authorities have little time to track down the criminal through the fraudulent site, which is often the best evidence available.[64] Once the site is shut down, the e-mail is the only remaining evidence, and phishers often cover their tracks using such tools as anonymous remailers.[65] Even if they can be found, the phishers are often not subject to U.S. jurisdiction. A study by the Anti-Phishing Working Group in October 2005 estimated that only 28.75% of phishing scams are launched from the United States.[66] California's legislature, however, relied on statistics showing that 78% of phishers

[58] John Leyden, *£6.5m Phishing Duo Jailed*, REGISTER (U.K.), June 28, 2005, at http://www.theregister.co.uk/2005/06/28/phishing_duo_jailed/ (stating that Havard's British accomplice received a four-year sentence).
[59] *See* Jonathan J. Rusch, Special Counsel, Dept. of Justice, Phishing and Federal Law Enforcement (Aug, 6, 2004), http://www.abanet.org/adminlaw/annual2004/Phishing/PhishingABAAug2004Rusch.ppt.
[60] H.R. Rep. No. 108-698, at 5 (2004), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:hr698.108.pdf ("[T]he most egregious abusers are seldom legitimate businesses or individuals who might be responsive to government regulation or civil penalties.").
[61] *See* Jeordan Legon, "*Phishing" Scams Reel in Your Identity*, CNN.COM, Jan. 26, 2004, http://www.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html ("Spammers mask their identities by using a wide array of computer servers, opening and closing their operations quickly and working outside the United States. All of this makes it more difficult for U.S. law enforcement to catch up with them.").
[62] APWG Jan. 2005 Report, *supra* note 43.
[63] APWG June 2006 Report, *supra* note 1.
[64] Peter Black, *Catching a Phish: Protecting Online Identity*, 8 INTERNET L. BULL. 133, 136 (2006).
[65] Michael Rustad, *Punitive Damages in Cyberspace: Where in the World Is the Consumer?*, 7 CHAP. L. REV. 39, 66 (Spring 2004).
[66] *See* ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT Oct. 2005), *available at* http://antiphishing.org/apwg_phishing_activity_report_oct_05.pdf..

were in the United States and that 15% of those were in California when it debated anti-phishing legislation in 2005.[67]

II. CALIFORNIA'S ANTI-PHISHING ACT

[14] In February of 2005, California State Senator Kevin Murray introduced Senate Bill 355.[68] The Bill, later named the Anti-Phishing Act of 2005, was passed by both the California Senate and the California Assembly in August 2005[69] and was signed by Governor Schwarzenegger in September 2005 to take effect in January 2006.[70] The Bill had the support of both Microsoft and the Consumer Technology Industry Association, a technology industry association.[71]

[15] Section 22948.2 of the new statute states:

> It shall be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by

[67] *Anti-Phishing Act of 2005: Hearing on S.B. 355 Before the S. Judiciary Comm.*, 2005-2006 Reg. Sess. (Cal. 2005), [hereinafter Apr. 5 Hearing] ("According to the FBI and the Internet Crime Complaint Center, 78 percent of all criminal "phishers" are located in the United States. Of these, 15 percent of all phishing scams originate in California, the most in the nation."). These statistics may simply have been out of date in a fast-changing area of technology. *See* Collier, *supra* note 45, at 19 ("Many of today's scams are operated beyond the reach of U.S. criminal prosecution. A year ago, most attacks were launched within the U.S.; today, two-thirds are launched from overseas. The Ukraine, Eastern Europe, Russia, Southeast Asia, and Africa are bastions of phishing.").

[68] S.B. 355, 2005–2006 Leg., Reg. Sess. (Cal. 2005).

[69] *Id.*

[70] *See* Press Release, Cal. Dep't of Consumer Affairs, New Laws Will Help Protect Against Identity Theft (Oct. 7, 2005) (http://www.dca.ca.gov/press_releases/2005/1007_idtheft.htm). This press release should be read with a grain of salt, since it erroneously states that "SB 355 makes the practice of Internet 'phishing' a crime in the state of California." *Id.* Senate Bill 355, of course, is not a criminal statute at all.

[71] *See* Apr. 5 Hearing, *supra* note 67 ("Microsoft contends that the '[s]trong laws and adequate enforcement' provided by SB 355 will be critical to addressing the phishing problem.").

> representing itself to be a business without the authority or approval of the business.[72]

[16] Three classes of persons may bring actions against violators of section 22948.2. The Attorney General or a district attorney may bring an actions against "a person who violates or is in violation of section 22948.2" for injunctive relief and to recover a civil penalty of up to $2,500 per violation.[73] An individual "who is adversely affected by a violation of section 22948.2 may bring an action, but only against a person who has directly violated section 22948.2."[74] The individual plaintiff may recover either three times actual damages or five thousand dollars per violation.[75] Most importantly, a "person who (A) is engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark, and (B) is adversely affected by a violation of section 22948.2" may sue for the greater of actual damages or five hundred thousand dollars.[76] This provision, unlike the provision for individuals, does not specify that the defendant must be a "direct violator" of section 22948.2. The fact that direct violators are specifically mentioned in the subsection referring to individuals, but not in the subsection referring to corporations, suggests that we must read the latter subsection as applying to both direct and indirect violators.

[17] The section of the statute regarding suits brought by the state does not define direct or indirect violation of section 22948.2, nor does it define the difference between violating and being in violation of.[77] Nothing in the legislative history gives any indication of an intent to impose liability on anyone other than the phishers.[78] There does not, however, seem to be any other way to read the plain language of the statute: with "direct" violation specifically required for individual plaintiffs but for no one else. The large statutory damage amount available to corporate plaintiffs,

[72] CAL. BUS. & PROF. CODE § 22948–22948.3 (West Supp. 2006).
[73] *Id.* § 22948.3(b).
[74] *Id.* § 22948.3(a)(2).
[75] *Id.*
[76] *Id.* § 22948.3(a)(1).
[77] *See id.* § 22948.3(b).
[78] The legislative history of the bill, including committee reports, is available at the California State Senate's website, http://info.sen.ca.gov/.

$500,000,[79] also hints at a defendant other than an individual phisher, particularly since many phishers are judgment-proof.[80] Though few commentators seem to have noticed, the Bill appears to have a broader reach than its press indicates. Secondary liability is a sort of stealth effect of the California Anti-Phishing Act.

[18] If a trademark holder, web page owner, or an ISP were to sue another ISP for indirectly violating, or being in violation of section 22948.2, the defendant would almost certainly attempt to take refuge in § 230 of the CDA,[81] which states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[82] The leading case interpreting § 230 is *Zeran v. America Online*, a negligence suit brought against an ISP for delays in removing messages after the plaintiff notified the ISP of the messages' defamatory content.[83] The *Zeran* court read § 230 as not only providing ISPs with immunity as publishers, but with distributor immunity as well.[84] Under the common law of defamation, a publisher is liable for dissemination of defamatory information even absent specific knowledge that the information was included in the published work.[85] A distributor, however, is liable only if he or she has

[79] CAL. BUS. & PROF. CODE § 22948.3(a)(1).
[80] *See* Stevenson, *supra* note 15, at 20.
[81] 47 U.S.C. § 230 (2000).
[82] *Id.* § 230(c)(2). The CDA defines "interactive computer service" broadly, as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." *Id.* § 230(f)(1). Courts have interpreted this definition to mean that the category of interactive computer services includes websites such as Matchmaker.com. *See* Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1065-66 (C.D. Cal. 2002); eBay, *see* Gentry v. eBay, Inc., 99 Cal. App. 4th 816, 831 (2002); and Amazon.com, *see* Schneider v. Amazon.com, 31 P.3d 37, 40-41 (Wash. Ct. App. 2001).
[83] *Zeran v. American Online Inc.*, 129 F.3d 327 (4th Cir. 1997).
[84] *Id.* at 332 ("Assuming *arguendo* that Zeran has satisfied the requirements for imposition of distributor liability, this theory of liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230.").
[85] PROSSER AND KEETON ON THE LAW OF TORTS, § 113, p. 810 (W. Page Keeton ed., 5th ed. 1984) ("Those who manufacture books by way of printing and selling them . . . are subject to liability as primary publishers because they have the opportunity to know the

actual knowledge of the defamatory statement.[86] By holding that § 230 applies both kinds of liability, the *Zeran* court broadened the statute's applicability, perhaps beyond what Congress intended.[87]

[19] Since *Zeran*, other courts throughout the country have interpreted § 230 to provide complete immunity for ISPs for the actions of third parties, not only for defamation but also for a range of other activities, "even if the service provider has actual knowledge of ongoing torts or crimes on its services."[88] For instance, in *Ramey v. Darkside Productions*, the D.C. District Court found that § 230 immunized an online adult entertainment guide against claims of intentional infliction of emotional distress, unjust enrichment, negligence, and fraud for using a woman's photograph without her permission, even though the ISP had actual notice that use of the photos infringed the woman's intellectual property rights.[89] In *Doe v. America Online*, the Supreme Court of Florida found that § 230 protected AOL from claims by a mother whose eleven-year-old son was featured in pornographic photographs and videotapes sold by the Defendant via AOL chat rooms, even though AOL had notice the Defendant was selling obscene photographs of a minor.[90] Further, in *Doe v. GTE.*, the Seventh Circuit found that under § 230 web hosting services had no secondary liability on sites they hosted for the sale of videotapes of athletes filmed

content of the material being published and should therefore be subject to the same liability rules as are the author and originator . . . .").

[86] RESTATEMENT (SECOND) OF TORTS § 581(1) (1977) ("[O]ne who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character.").

[87] *See* Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 1395 (2004), *cert. granted*, 87 P.3d 797 (2004) ("The view of most scholars who have addressed the issue is that *Zeran*'s analysis of section 230 is flawed, in that the court ascribed to Congress an intent to create a far broader immunity than that body actually had in mind or is necessary to achieve its purposes."); *see also* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 371–73 (2005) ("An activist judiciary . . . has radically expanded § 230 by conferring immunity on distributors . . . . Courts have conflated distributors' liability with publishers' liability, blithely ignoring distinctions developed over centuries of tort law.").

[88] Rustad & Koenig, s*upra* note 87, at 370.

[89] Ramey v. Darkside Productions, No. 02-730, 2004 U.S. Dist. LEXIS 10107, at *12, *20 (D.D.C. May 17, 2004).

[90] Doe v. American Online Inc., 783 So. 2d 1010, 1017-18 (Fla. 2001).

without their permission while showering.[91] The judiciary's broad interpretation of § 230 "has resulted in an inhospitable legal environment for consumers in cyberspace."[92]

[20] There are, however, indications that California could become a friendlier environment for plaintiffs seeking to establish tort liability against ISPs. Initially California's courts followed the *Zeran* reasoning. In *Stoner v. eBay*, a California Superior Court held that the Defendant could not be liable for its users' sale of bootleg recordings, even if eBay had knowledge or notice that the recordings infringed intellectual property rights.[93] The case cites *Zeran* favorably,[94] and follows its reasoning. A more recent California decision, *Barrett v. Rosenthal*, however, suggests that at least some of the state's judges may be rethinking the broad view of ISP immunity under the CDA.[95]

[21] *Barrett* is a defamation case in which two physicians sued a woman who posted a message to Usenet newsgroups calling them "quacks" and accusing one of them of stalking a Canadian radio personality.[96] The trial court determined that the latter accusation was a provably false statement of fact, but that the defendant had merely republished the information and thus was immune from liability under the CDA.[97] The appellate court reversed, specifically repudiating *Zeran* and finding that Congress was aware of the traditional distinction between publishers and distributors. According to the appellate court, if Congress had "intended Section 230 to immunize providers and users not merely from primary publisher liability but also from distributor liability, it would have made this clear."[98] The court went on to note that the imposition of distributor liability would not require an ISP to screen postings in advance, but only "to act reasonably

[91] Doe v. GTE Corp., 347 F.3d 655, 659–60 (7th Cir. 2003) (noting the plaintiff did not allege that GTE had notice of the activity in question).
[92] Rustad & Koenig, *supra* note 87, at 373.
[93] Stoner v. eBay, 2000 WL 1705637, 1854 (2000).
[94] *Id.*
[95] *Barrett*, 9 Cal. Rptr. 3d at152.
[96] *Id.* at 145–46.
[97] *Id.* at 146.
[98] *Id.* at 154 (pointing out that "while federal circuit court precedence on issues of federal law is certainly entitled to substantial deference, it is not binding." (quoting Yee v. City of Escondido, 224 Cal. App. 3d 1349, 1351 (Cal. Ct. App. 1990))).

after being placed on notice that the communication is defamatory."[99] The *Barrett* court noted that its repudiation of *Zeran* did not conflict with two previous cases that relied on *Zeran*, *Gentry v. eBay*[100] and *Kathleen R. v. City of Livermore*,[101] since in both of those cases the defendants would not have been liable as distributors under the common law.[102]

[22] The California Supreme Court has granted review of *Barrett v. Rosenthal*, [103] and oral arguments were presented on September 5, 2006.[104] The court will issue its opinion on December 4, 2006.[105] In the meantime, the Court of Appeal's opinion cannot be cited as precedent.[106] Yet the prospect of imposition of distributor liability has caused some alarm among ISPs and other providers of online services. Amicus briefs were filed by eBay [107] and by a consortium of online services and content providers[108] that includes AOL, Microsoft, Google, CNN, and the Newspaper Association of America (NAA). The NAA is particularly worried that California will attract forum-shopping plaintiffs who would have no cause of action in any other jurisdiction.[109]

[23] If the California Supreme Court rules in Barrett's favor and holds that the reasoning of the *Zeran* court is no longer considered persuasive in California courts, then liability could be imposed on ISPs if they have

[99] *Id.* at 163.
[100] *Gentry*, 99 Cal. App. 4th at 828-29, 835.
[101] Kathleen R. v. City of Livermore, 87 Cal. App. 4th 684, 695 (Cal. Ct. App. 2001).
[102] *Barrett*, 9 Cal. Rptr. 3d at 154 n.9.
[103] *Barrett*, 87 P.3d at 797.
[104] For an eyewitness account of the oral arguments, see Colette Vogele, Entry Archive: Cal. Supreme Ct. to Hear Section 230 Case Today, Sept. 5, 2006. http://cyberlaw.stanford.edu/blogs/vogele/archives/004094.shtml.
[105] *Id.*
[106] *Barrett*, 87 P.3d at 797.
[107] Brief for eBay as Amicus Curiae Supporting Respondent, Barrett v. Rosenthal, No. S122953, 2004 WL 3256403 (2004).
[108] Brief for Amazon.com, Inc., et al. as Amici Curiae Supporting Respondent, Barrett v. Rosenthal, No. S122953, 2004 WL 3256404 (2004) [hereinafter Amazon et al. Brief].
[109] *See* Newspaper Ass'n of Am., Public Policy News, Feb. 2005, http://www.naa.org (follow "Publications" hyperlink; then follow "NAA Public Policy News" hyperlink; then follow "Next" hyperlink; then follow "NAA Public Policy News, Feb. 2005" hyperlink) ("The NAA brief argues the court of appeal's decision will create confusion on an issue that warrants a nationwide solution and will permit California's courts to become a haven for forum-shopping plaintiffs.").

knowledge that their facilities are being used for third party tortious activity, but fail to act to stop such activity.[110] In such an environment, an ISP that had not taken steps to take down a phishing website or to cut off a phisher's e-mail access after receiving notification could conceivably be found to be indirectly in violation of section 22948.2 of the Anti-Phishing Act.[111]

[24] One clue that the California legislature could not have had such secondary liability in mind when it drafted the Anti-Phishing Act is the involvement of Microsoft in the Bill's passage.[112] Indeed, Microsoft has been a proponent of anti-phishing legislation around the country[113] and has filed 117 Lanham Act lawsuits against John Doe phishers, hoping to use discovery to determine their identities.[114] Yet Microsoft would probably not be in favor of using secondary liability against ISPs. The corporation operates its own internet service provider, the Microsoft Network (MSN).[115] Microsoft is an amicus curiae on the side of the respondent in the *Barrett v. Rosenthal* appeal, arguing that § 230 should continue to be construed to apply to publishers and distributors alike.[116] It is unlikely that Microsoft's lawyers would be advocating for ISP immunity in one

[110] *See* Rustad & Koenig, *supra* note 87, at 381–82 ("This case may well be a bellwether decision that will reshape online intermediary law . . . . A decision by the Supreme Court of California that downsizes § 230 would open the door to a greatly needed radical reconsideration of the duty of care in cyberspace.").
[111] CAL. BUS. & PROF'L CODE § 22948.2 (West Supp. 2006).
[112] *See* Apr. 5 Hearing, *supra* note 67.
[113] *See* Mike Sunnucks, *Microsoft Seeks to Stop "Phishing" Expeditions*, BUS. J. OF PHOENIX, Jan. 7, 2005, http://phoenix.bizjournals.com/phoenix/stories/2005/01/10/story4.html.
[114] Brian Krebs, *Microsoft Seeks to Identify Phishing Scam Authors*, WASHINGTONPOST.COM, Mar. 31, 2005, http://www.washingtonpost.com/wp-dyn/articles/A16257-2005Mar31.html. (describing Microsoft's victory in one such case, in which it obtained a three million dollar judgment on Lanham Act claims against a 21-year-old Iowa resident named Jayson Harris who had used his grandfather's computer to set up a phishing scam). Harris now faces a 75-count criminal indictment in federal court. *See* Ann McGlynn, *Internet-Fraud Hunt Leads to QC*, QUAD-CITY TIMES (Iowa), Aug. 23, 2005, http://www.qctimes.net/articles/2005/08/23/news/local/doc430ab1f682634754831798.txt.
[115] Microsoft Network Home Page, http://www.msn.com (last visited Sept. 13, 2005).
[116] Amazon et al. Brief, *supra* note 108.

situation and for secondary liability on the other.[117] Still, whether or not the statute's wording was intentional, and whether or not Microsoft's lawyers noticed, California's anti-phishing statute could potentially be read to impose secondary liability on ISPs which fail to take affirmative steps when notified that their resources are being used by phishers.

III. Is Imposing Secondary Liability on ISPs a Practical Way to Deter Phishing?

[25] If the California Supreme Court affirms the Appellate Court's reasoning in *Barrett*, a corporation harmed by a phishing attack (say, a financial institution required to make good on fraudulent credit card charges) could sue an ISP as a distributor for actual or statutory damages under section 22948.3(a)(1) of California's Anti-Phishing Act.[118] The first such lawsuit could be an interesting test case. The ISP would likely argue that it is neither a publisher nor a distributor, but a mere conduit. Under the common law of defamation, there is no liability for conduits,[119] which have no duty to pre-screen or remove messages.[120] The conduit argument might succeed as applied to the phishing e-mails, but would be considerably less convincing in regard to phishing websites, which are active for multiple days and which the provider of hosting services could easily find and remove upon notice. It is entirely possible that a court could find distributor liability, under an affirmed *Barrett*, for an ISP that failed to shut down phishing websites.

---

[117] It is, however, likely that Microsoft would escape distributor liability under the Anti-Phishing Act given its own proactive behavior in going after phishing. Still, even the most anti-Microsoft conspiracy theorist would find far-fetched the suggestion that Microsoft supported the Anti-Phishing Act in the hope that it would impose secondary liability on other, less careful ISPs.

[118] CAL. BUS. & PROF'L CODE § 22948.3(a)(1) (West Supp. 2006).

[119] *See* Anderson v. N.Y. Tel. Co., 35 N.Y.2d 746, 750 (1974) ("The telephone company is not part of the "media" which puts forth information after processing it in one way or another. The telephone company is a public utility which is bound to make its equipment available to the public for any legal use to which it can be put . . . . ").

[120] *See* Lunney v. Prodigy Servs. Co., 94 N.Y.2d 242, 249 (1999)("[A]n ISP, like a telephone company, is merely a conduit . . . . [W]e are unwilling to deny [the defendant] the common-law qualified privilege accorded to telephone and telegraph companies. The public would not be well served by compelling an ISP to examine and screen millions of e-mail communications, on pain of liability for defamation.").

[26] Given the unresolved status of the *Barrett* case, the prospect of such liability being imposed is so hypothetical that the mere possibility is not enough to force ISPs to undertake steps to stop phishing attacks before they occur. This seems a shame, since ISPs are almost certainly the least cost avoider for phishing attacks.[121] Given notice, they can shut down the phisher's website and internet access quickly and completely. Even absent notice, they may be able to devise ways to prevent phishing attacks from ever occurring.[122] However, ISPs currently have no duty to take such steps, nor a duty to cooperate with plaintiffs seeking information about phishers' identities. [123] Using secondary liability to force ISPs to take steps to prevent injuries to customers and other corporations, steps they would otherwise have no incentive to take, seems such an ingenious solution to the phishing problem that it is almost disappointing to conclude that such a result was probably not intended by California legislators.

[27] Of course, social problems do not always require legal solutions. Problems can be solved extralegally through technological or market means.[124] Indeed, in the case of phishing, extralegal solutions may be far

[121] *See* Rustad & Koenig, *supra* note 87, at 339 ("ISPs are generally in the best position to mitigate damages from online fraudulent schemes, website defamation, and other information-based torts by taking down objectionable content."); *id.* at 390–91 (noting that ISPs can install spam filters, identify computer intrusions, develop comprehensive identification systems, and maintain audit trails).

[122] Microsoft, for instance, has contracted to purchase data on an ongoing basis from third-party vendors on phishing threats and known phishing sites. This data will be used by Microsoft's Phishing Filter, which is currently downloadable as part of the MSN Search toolbar, and by the new Internet Explorer 7. Gregg Keizer, *Microsoft Goes Outside for Phishing Help*, INFO. WK., Nov. 17, 2005, http://www.informationweek.com/shared/printableArticle.jhtml?articleID=174300997. However, the move is controversial; privacy advocates oppose the Phishing Filter since it sends user data to Microsoft and potentially gives Microsoft power to decide what sites are safe. Mike Ingram, *Microsoft Anti-Phishing Software Raises Internet Privacy Concerns*, WORLD SOCIALIST WEB SITE, Sep. 17, 2005, http://www.wsws.org/articles/2005/sep2005/micr-s17.shtml ("There is a very real danger that the phishing filter will have the effect of creating a two-tier Internet, with sites designated as safe or not, supposedly on the basis of the number of people visiting them on a list controlled by the world's largest software corporation.").

[123] Rustad & Koenig, *supra* note 87, at 383 ("Not only are ISPs immune from lawsuits for hosting or posting third part content, but they also have no legal duty to cooperate with the plaintiff in tracking down cybercriminals.").

[124] *See* Lawrence Lessig, *Preface to a Conference on Trust*, 81 B.U. L. REV. 329, 329 (2001). Elsewhere, Lessig distinguishes between "East Coast Code," that is, statutes, and

more promising than the law.[125] So far, neither criminal nor civil law seems to have much effect against the direct infringers, the phishers themselves.[126] Extralegal solutions to phishing include technological fixes (either by the ISPs or by the large corporate targets of phishing) and consumer education. Many web-based businesses are attempting to educate their customers not to give out information,[127] but there are signs that the message has not yet been widely received.[128] However, new state anti-phishing laws may be indirectly effective by increasing public awareness of phishing scams.[129] Customers can even fight phishing directly: one commentator offers a more devious way for consumers to hoist phishers by their own petard:

> If everyone who received phishing e-mails replied with false information, the criminal would be forced to cull through a million replies to get at the 100 with useful information. While this requires the user taking time to fill

"West Coast Code," "the instructions embedded in the software and hardware that make cyberspace work." *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 53 (1999).

[125] *See* Stevenson, *supra* note 15, at 1 ("[A]lthough the Anti-Phishing Act can play a supporting role in the battle, technological solutions are the most effective means of reducing or eliminating phishing attacks.").

[126] Microsoft's use of trademark law and John Doe lawsuits to pursue phishers may be more effective than previous methods. *See supra* note 115 and accompanying text. While it is unlikely that Microsoft will be able to collect its three million dollar judgment against Jayson Harris, the technique may help Microsoft find United States-based phishers, who can then be prosecuted criminally.

[127] Press Release, TRUSTE, For the First Time, Security, Financial, E-Commerce and Government Sectors Gather to Build Nationwide Consumer Education Program to Fight Phishing Attacks (June 13, 2005), *available at* http://www.truste.org/cgi-dada/mail.cgi?flavor=archive&id=20050614185052&list=Press_Releases.

[128] Press Release, National Cyber Security Alliance, One in Four Computer Users Hit by Phishing Attempts Each Month, According to Major In-Home Computer Safety Study (Dec. 7, 2005), *available at* http://www.staysafeonline.info/news/press_dec07_2005.html (presenting survey findings that only 42% of those surveyed were familiar with the term "phishing," and only 57% of those familiar with it could define it).

[129] *See* Koprowski, *supra* note 17 (quoting an executive at a data security firm as saying, "[t]he anti-phishing law will help raise awareness for consumers, but otherwise will be of little impact in increasing the number of phishers that will be prosecuted").

> out the forms, it would increase labor exponentially for the phisher, greatly reducing the profitability of the scam.[130]

[28] Both legal and extralegal techniques have roles to play in fighting online fraud. If secondary liability is an effective solution to the phishing problem, its value will be in providing ISPs with an incentive to reduce their own liability by developing technological fixes.

[29] But ISPs are not the only parties who can offer a technological solution. The corporate victims of phishing already have incentive to create technological barriers to phishing. Phishing causes them both direct financial loss and erosion of their customers' trust.[131] It may seem unreasonable for the customers to blame the corporations for the security breach, since the customers themselves are giving away the information. But con artists on the internet, unlike those on the street, may exploit security choices made by the corporations in setting up their websites.[132] By changing those security choices, banks and other institutions doing business online may be able to foil the phishers.[133]

---

[130] Kerstein, *supra* note 8 (quoting Robert X. Cringely, a columnist for PBS and Infoworld).

[131] *See* FDIC Report, *supra* note 38, at 14 ("Some analysts . . . have suggested that the rapid rise in phishing attacks is threatening consumer confidence and that diminished consumer trust in online transactions will hurt all participants in Internet commerce."); *see also* Jeanette Borzo, *Something's Phishy: Online Identity Theft Scams Are So Effective That They Threaten to Steal a Vital Ingredient of E-Commerce: Trust*, WALL ST. J., Nov. 15, 2004 (discussing potential erosion of consumer confidence caused by phishing).

[132] *See* Smedinghoff, *supra* note 40, at 2 (suggesting that the approach to information security taken by the spoofed company may somehow contribute to the success of the attack).

[133] Some commentators have suggested that banks, like ISPs, do not have sufficient incentive to spend money on heightened security:

> Financial institutions have no incentive to reduce those costs of identity theft because they don't bear them. Push the responsibility ,all of it, for identity theft onto the financial institutions, and phishing will go away . . . . It will go away because the information a criminal can get from a phishing attack won't be enough for him to commit fraud - because the companies won't stand for all those losses.

Bruce Schneier, *A Real Remedy for Phishers*, WIRED NEWS, Oct. 6, 2005, at http://www.wired.com/news/politics/0,1283,69076,00.html.

[30] One obvious security weakness is the use of a single password as a user's only form of identification. Thieves thus need only one piece of information to break into a bank account. Requiring an additional piece of information, "two-factor identification," is one potential solution.[134] Another is the Trusted Platform Module (TPM) chip,[135] a tiny security chip that is assigned a unique, permanent, and unchangeable identifier before the computer in which it is installed leaves the factory. If your bank has TPM-reading software, it will allow you website entry with your password only if you are also using your own computer with its unique TPM code.[136]

[31] Other technological solutions include scanning software which patrols the internet for phishing sites using someone else's trademarks and slogans[137] and a form of Caller ID for e-mail[138] that would allow ISPs to make sure that incoming e-mail was in fact from the entity it pretended to be from.[139] But these technological solutions cost money, and online businesses and banks may not have sufficient incentive to spend that money absent regulation. As one commentator notes:

---

[134] *See* FDIC Report, *supra* note 38, at 26 ("[A]lmost all phishing scams in use today could be thwarted by the use of two-factor authentification."). Two-factor identification combines factor one, a password, with factor two, either biometric information (such as fingerprints, eye scans, or a voice read) or a token (such as a USB device that plugs into the user's computer's USB port, or a smart card inserted into a reader). Systems protected by two-factor identification are far less vulnerable to phishers. *Id.* at 26–28.

[135] *See* Rogers, *supra* note 31.

[136] *See id.* (stating that while TPM chips are currently installed mostly in computers belonging to large corporations, they will be installed in many consumer models beginning in 2006).

[137] FDIC Report, *supra* note 38, at 22–24.

[138] Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-Mail Advertising*, 10 VA. J.L. & TECH. 5, at 39 (2005). The Caller ID for e-mail approach was proposed by Microsoft. *Id.* eBay and Earthlink use forms of Caller ID in their downloadable toolbars to alert customers to potentially fraudulent sites. Borzo, *supra* note 131.

[139] *See id.* at 39–40. Caller ID for e-mail would do little to stop spam that emanates from domains and servers considered to be legitimate, but it could weed out e-mails with forged "from" addresses. *See id.* at *42. Yahoo has a similar system, DomainKeys, a cryptographic system that allows ISPs to verify the sender of incoming e-mails. *Id.* at 53–57.

> Financial institutions have no incentive to reduce those costs of identity theft because they don't bear them. Push the responsibility—all of it—for identity theft onto the financial institutions, and phishing will go away. . . . It will go away because the information a criminal can get from a phishing attack won't be enough for him to commit fraud—because the companies won't stand for all those losses.[140]

[32] Websites and ISPs are the obvious technological line of defense against phishing—they can take global steps which most customers cannot take. But absent liability, they may be reluctant to take on the expense. Secondary liability is one way to spur the development of security technology. If, however, the government did attempt to impose secondary liability directly through legislation, it would face a great deal of opposition from the online industries.

IV. CONCLUSION

[33] The California legislature almost certainly did not intend to include secondary liability for ISPs in its Anti-Phishing Act. But if the California Supreme Court affirms the lower court's rejection of the *Zeran* reasoning and finds that § 230 of the CDA does not preclude distributor liability, then a court could conceivably find such liability. ISPs can be a powerful ally in the fight against phishing, but the threat of secondary liability would need to be substantial before it would induce ISPs to introduce more substantial anti-phishing measures. The larger ISP operators such as AOL and Microsoft, who are likely to be the victims of phishers as well as their enablers, will probably be at the forefront of any such developments. Absent secondary liability, though, smaller ISPs will have little incentive to take steps against phishers even when phishing is reported to them.

[34] Other tools such as ongoing consumer education and increased security by the banks and websites whose customers are most likely to be targets of phishing attacks may be more effective against phishing than any sort of legal liability. Yet the possible addition of secondary liability to the arsenal of those fighting against phishing could convince the ISPs,

[140] Bruce Schneier, *A Real Remedy for Phishers*, WIRED NEWS, Oct. 6, 2005, at http://www.wired.com/news/politics/0,1283,69076,00.html.

who are probably the least cost avoider in the prevention of phishing attacks, to become more active in the fight against phishing.