Sotelo v. Directrevenue, LLC: Paving the Way for Spyware-Free Internet

Julie Anderson

David Fish

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation
Julie Anderson and David Fish, Sotelo v. Directrevenue, LLC: Paving the Way for Spyware-Free Internet, 22 SANTA CLARA HIGH TECH. L.J. 841 (2005).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol22/iss4/6
SOTELO V. DIRECTREVENUE, LLC: PAVING THE WAY FOR A SPYWARE-FREE INTERNET

Julie Anderson & David Fish†

"Many companies and computer users consider pop-up advertisements and Spyware an Internet scourge"‡

INTRODUCTION

Consumers who wish to connect to the Internet have had to pay a high price lately for doing so. The high price has not necessarily come in the form of Internet connection bills, but in the form of wasted time and diminished computer productivity that is caused from pop-up advertisements frequently appearing on consumers’ computers. A pop-up advertisement is an advertisement that is displayed on the user’s computer through a new browser window. Because it appears through a new browser window, the advertisement cannot be removed unless the user interrupts his or her work to close or minimize the display. This form of advertising has gained popularity with advertisers, but has generated much ill-will with consumers. The pop-up advertisements are distributed through spyware software programs,¹ which generally track the user’s Internet activity and send a flood of these pop-up advertisements to the user’s computer. These spyware programs are often downloaded onto the computer without the user’s knowledge or consent. Once downloaded, the excessive

† Julie Anderson and David Fish are both employed at The Collins Law Firm, P.C. in Naperville, Illinois. The Collins Law Firm is currently representing plaintiff Mr. Stephen Sotelo in Sotelo v. DirectRevenue, LLC.


¹ Spyware is defined as “any software that covertly gathers information about a user while he/she navigates the Internet and transmits the information to an individual or company that uses it for marketing or other purposes.” WEBSTER'S NEW MILLENNIUM DICTIONARY OF ENGLISH, (Barbara Ann Kipfer ed., preview ed. v. 0.9.6 2005), available at http://dictionary.reference.com/search?q=spyware. This article does not intend to suggest that DirectRevenue is a spyware company. Rather, it reports on the allegations of the Sotelo complaint that was filed in 2005.
number of pop-up advertisements that are sent drain a user's computer capacity and interrupt the user's work and Internet activity.

This article will provide an in-depth look into *Sotelo v. DirectRevenue, LLC*, a recent case brought on behalf of computer users against alleged participants in this spyware industry. *Sotelo v. DirectRevenue, LLC* was the first case in which a federal court held that an individual computer user could state a claim against an alleged spyware software company, along with the advertisers and agencies doing business with the spyware company. Part I of this article provides a brief background of the spyware industry; Part II discusses the case law that preceded *Sotelo v. DirectRevenue, LLC* and created a strong foundation for the viability of a trespass to chattels cause of action. Part III will discuss the complaint the plaintiff filed in *Sotelo v. DirectRevenue, LLC*, and Part IV analyzes the court's ruling on defendants' motions to dismiss the plaintiff's complaint. Part V discusses the sweeping injunctive relief that DirectRevenue agreed to in its settlement of the lawsuit. Finally, Part VI discusses how the *Sotelo* case stood on stronger footing than previous spyware cases, to ultimately achieve greater success than what was realized in these earlier cases.

I. THE SPYWARE INDUSTRY

Last year alone, consumers spent $143.2 billion on online transactions. With the stakes of online business so high, companies are looking for more creative ways to attract consumers' attention and business to their web pages. Online advertising first began with banner advertisements and spam e-mails. Banner advertisements were stationary ad displays that could be seen on the side or the top of a web page, and spam was unsolicited bulk e-mail that was sent to a computer user's e-mail account. However, as banner advertisements were typically ignored and spam e-mail was deleted without consumers ever reading it, advertisers looked for more creative ways to grab the consumers' attention—and with that idea, the pop-up advertisement was born.

---


4. *Id.*

A pop-up advertisement is an advertisement that is displayed on a new browser window. Often a user will not be able to use their computer until some action is taken to close or minimize the pop-up window. Pop-up advertisements are frequently sent by utilizing spyware that has been installed on a computer. These spyware programs are bundled into free software programs (such as games or screen savers) and downloaded onto a user’s computer, often without a user’s consent. The spyware software will then track the Internet activity and apparent interests of the user, and pop-up advertisements that are targeted towards these tracked interests are then sent to the user’s computer. For example, if a computer user who has spyware software downloaded onto his or her computer was interested in browsing travel-related websites, the spyware software could monitor the travel-related interests of the browsing behavior and send advertisements to the computer from other travel-related companies who had paid the spyware software company to have access to this Internet advertising service.

The “advantage” that businesses receive from the pop-up ads is that, unlike the banner ads or spam e-mail which can easily be ignored, the pop-up is automatically displayed on the computer screen and cannot be removed unless the user manually closes the browser window on each advertisement that is displayed. These advantages of the pop-up ads extend only to advertisers, however, they are generally despised by consumers.

II. CASE LAW THAT PAVED THE WAY FOR SOTELO V. DIRECT REVENUE, LLC

Before spyware advertising became popular, both computer users and Internet Service Providers (ISPs) experienced frustrations with the earlier Internet advertising practice of spam e-mail. The mass

---

7. Wilson, supra note 3, at 570 ("[W]hen a pop-up ad pops up, users are forced to stop whatever they are doing and close the newly created browser window.").
11. Morrissey, supra note 10; McDermott, supra note 8.
amounts of unsolicited e-mails took up much of the limited storage space available on Internet Service Providers’ servers and the users’ inbox memory. Computer users were also growing tired of sifting through the unwanted e-mails each day, and Internet Service Providers were spending more time and resources fielding complaints from unhappy customers and attempting to build filters that would block out the unwanted mail. The frustrations from both the consumers and Internet Service Providers led to legal action against the companies sending the spam e-mail. The cases that first attacked spam e-mail found that one of the oldest torts, trespass to chattels, was perhaps the most effective weapon to combat the modern problems associated with Internet interference.

The first significant decision in this area was *CompuServe v. Cyber Promotions*. CompuServe was an Internet Service Provider that had received numerous complaints from customers who were receiving unwanted e-mails from Cyber Promotions. Plaintiff demanded that Cyber Promotions stop sending the unwanted e-mails to CompuServe’s customers, but this demand was ignored. CompuServe had tried developing software that could block the unwanted e-mails, but its efforts were insufficient, and the company kept on losing customers who were frustrated by the number of unwanted e-mails they continued to receive. In court, CompuServe requested a preliminary injunction to prevent the defendant from sending additional e-mails. CompuServe alleged that the conduct of CyberPromotions constituted trespass to chattels, and the court agreed. The court found that “electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action,” and “to the extent that

13. Id.
17. Id. at 1017.
18. Id. at 1019.
19. Id. at 1017.
20. Id. at 1021.
defendants’ multitudinous electronic mailings demand disk space and drain the processing power of plaintiff’s computer equipment, those resources are not available to serve CompuServe subscribers[, and] therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendant’s conduct.”  

Similar cases (brought by Hotmail and America Online) followed the reasoning behind the CompuServe decision—to also hold that a company that interferes with the use and enjoyment of one’s computer through sending excessive numbers of unauthorized e-mail, damages the chattel. The sender can then be liable to the owner of the computer for trespass to chattels.

However, the use of a trespass to chattels claim to establish liability against senders of unwanted e-mails is not without limitations. Some guidelines on the cause of action were established in Intel v. Hamidi, another significant decision in the area of Internet-related case law. In Intel v. Hamidi, the defendant (a former employee of Intel Corporation) had sent e-mails to Intel employees that criticized Intel’s employment and hiring practices. These e-mails were sent only approximately six times over a period of two years. Intel attempted to characterize the defendant’s conduct as a trespass to chattels upon its computers and computer system, but this argument was rejected by the court. Although the e-mails were unwanted, the court reasoned that a claim for trespass to chattels could not be established if the e-mails had not damaged Intel’s computers or impaired their functioning or productivity in any way. The damage that Intel had really suffered was not related to the computer (the chattel that formed the basis of the claim), but the loss of productivity from employees who read and later discussed the contents of the defendant’s critical e-mails. CompuServe and Intel, taken together, establish that so long as the computer (or chattel) itself

21. Id. at 1022.
24. Intel, 30 Cal.4th at 1346, 1 Cal. Rptr. 3d at 36, 71 P.3d at 299.
25. Id.
26. Id. at 1347, 1 Cal. Rptr. 3d at 36, 71 P.3d at 300.
27. Id.
has been impaired or damaged as a result of the unwanted e-mails, a claim for trespass to chattels can be established.\textsuperscript{28}

Other Internet interferences besides spam e-mail have also been successfully attacked through trespass to chattels. In \textit{eBay v. Bidder's Edge}, the final significant Internet-related decision discussed in this article, the defendant employed a computer "web crawler" that continuously searched eBay’s online auction web page.\textsuperscript{29} The web crawler would copy information from eBay’s web site and post that information on defendant’s own web page.\textsuperscript{30} Defendant’s program performed an average of 10 million searches per day upon eBay web site, and damaged eBay’s computer system through consuming approximately 1.53% of the available server space.\textsuperscript{31} The court followed the reasoning of \textit{CompuServe}, and found that Bidder's Edge would likely be liable as a trespasser for the damage its web crawler caused to eBay’s computers. This case is significant because it demonstrates that trespass to chattels is not limited to the spam e-mail cases where it was first used.\textsuperscript{32} A computer that is damaged through any interference can establish a claim for trespass to chattels against the person or entity that caused the damage.

These cases have established a strong foundation that when unwanted interferences of any type damage a computer by "demand[ing] the disc space and drain[ing] the processing power" of the plaintiff’s computer equipment, a cause of action for trespass to chattels can be established.\textsuperscript{33} Just as the unwanted e-mails and web crawler damaged the computer systems in the previous cases, the unwanted pop-up advertisements have similarly damaged Mr. Sotelo's computer, and the foundation provided from these decisions has paved the way for Mr. Sotelo’s complaint.

\textsuperscript{28} Siebecker, \textit{supra} note 15, at 929.
\textsuperscript{30} \textit{eBay}, 100 F. Supp. 2d. at 1060-62.
\textsuperscript{31} \textit{Id.} at 1064.
\textsuperscript{32} \textit{See also} \textit{Register.com, Inc. v. Verio, Inc.}, 126 F. Supp. 2d 238, 248-51 (S.D.N.Y. 2000).
III. SOTEO’S COMPLAINT

A. Parties

On March 31, 2005, a five-count class action complaint was filed against multiple defendants who were alleged to either be involved in the spyware industry, or who allegedly advertised through those in the spyware industry. The defendants included, AccuQuote, BetterInternet, aQuantive, DirectRevenue, DirectRevenue Holdings, and numerous “John Does” which were identified as other entities or individuals who were also involved in the wrongdoing, and would be named as a formal defendant once their identities were ascertained.34

B. DirectRevenue’s Product

The factual basis of the complaint alleged that DirectRevenue consistently engaged in deceptive conduct by “secretly installing its software onto computers” by bundling the unwanted spyware software into other more desirable and legitimate software programs that the user can download for “free” (e.g., video games).35 When a user downloads the “free” program, the spyware software is also alleged to unknowingly download onto the computer without the user’s knowledge or, frequently, his or her consent.36

DirectRevenue does have an End User Licensing Agreement that explains the terms of the downloaded software; however, the complaint alleged that this agreement is frequently not seen by the user for different reasons.37 For example, a user who has Microsoft

---

34. Complaint for Plaintiff at ¶ 1-5, Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219 (N.D. Ill. 2005) (No. 05 C 2562).
35. Karen D. Schwartz, Spyware Lawsuit Alleges Computer Hijacking, EWEEK, Apr. 5, 2005, http://eweek.com/article2/0,1759,1782649,00.asp (“Sometimes ... the way [DirectRevenue] goes about its business is downright offensive.”). Susan Kuchinskas, Analyst Claims the Web Giant Supports Spyware Companies with its Pay-Per-Click Ads, ESECURITY PLANET, Sept. 1, 2005, http://esecurityplanet.com (“DirectRevenue has the worst practices. It may use misleading pop-ups to get users to install it, and it's unusually difficult to remove ... it can disable and delete other software on a user’s PC.”); Brad Stone, Is This Software on Your Hard Drive?, NEWSWEEK, Dec. 12, 2004 (“Industry watchers familiar with [DirectRevenue] say it has stooped as low as any of its rivals in the practices it uses to distribute its software.... Consumer advocates familiar with the company charge that DirectRevenue has engaged in an array of unethical practices.”).
36. Kuchinskas, supra note 35 (“DirectRevenue has the worst practices. It may use misleading pop-ups to get users to install it, and it's unusually difficult to remove ... it can disable and delete other software on a user’s PC.”).
Windows Pack 2 (a security feature) installed on his or her computer, a message pops up as the spyware is being downloaded that asks if the user wants "to install this software." See figure below.

![Internet Explorer Security Warning]

This message does not even mention spyware, and is inherently misleading for the user that does want to install the "free" software such as the game. The message is also confusing because the "name" of the software provided in the warning is not even an intelligible sentence, yet this is the only link available to view the End User Licensing Agreement on this screen.

Once installed, DirectRevenue’s software allegedly tracks the user’s Internet activity and overwhelms the computer with unsolicited pop-up advertisements. The pop-up advertisements will appear in a new browser window over the computer screen that the user was previously viewing. The pop-up will generally remain on the computer screen until the user closes the browser window. The lawsuit alleged that the pop-up advertisements sent through spyware cause more than mere inconvenience because they flood a user’s computer in such high numbers and at such a high rate that it causes serious disruptions to the user’s work. Newsweek reported that

38. _Id._
39. _Id._
40. _Id._ at 16.
41. _Id._ at 18.
42. _Id._ at 20.
DirectRevenue may have sent as many as 1.5 billion pop-up advertisements in just one month of business.\textsuperscript{43}

The complaint alleged that the rapid influx of pop-up advertisements is frustrating to the computer user and causes strain on the machine itself: such as causing the computer to slow down, taking up bandwidth over the Internet connection, using memory on the computer, and utilizing pixels and screen space on the monitor.\textsuperscript{44} These programs also decrease a user's productivity as a user must spend a great amount of time closing the browser windows for the continually appearing pop-up advertisements and waiting for the slowed down machine to operate.\textsuperscript{45}

The lawsuit further alleged that user's frustrations are further exacerbated by the difficulties encountered in removing the spyware program from the computer. For example, \textit{Newsweek} reported that DirectRevenue has "changed its name so often that frustrated users can't find the company to complain."\textsuperscript{46} Likewise, the complaint alleged that DirectRevenue also changes the file name of its software to prevent anti-spyware programs and computer technicians from locating the program and removing it from the computer.\textsuperscript{47}

\textbf{C. Legal Claims}

The plaintiff's complaint alleged that this deceptive activity fell within five legal causes of action.

First, plaintiff's complaint alleged that all defendants should be liable for their actions through trespass to chattels.\textsuperscript{48} Trespass to chattels is a very antiquated tort that has recently reemerged to combat the very modern problems associated with interference to a computer.\textsuperscript{49} Illinois law is unclear on the elements of the tort, but the Restatement recognizes the tort and defines it as follows:

\begin{itemize}
\item \textsuperscript{43} Stone, \textit{supra} note 35.
\item \textsuperscript{44} Complaint for Plaintiff at ¶ 20, Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219 (N.D. Ill. 2005) (No. 05 C 2562).
\item \textsuperscript{45} \textit{Id}.
\item \textsuperscript{46} Stone, \textit{supra} note 35.
\item \textsuperscript{47} Complaint for Plaintiff at ¶ 12, Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219 (N.D. Ill. 2005) (No. 05 C 2562).
\item \textsuperscript{48} \textit{Id} at ¶¶ 29-30.
\item \textsuperscript{49} Wilson, \textit{supra} note 3, at 578 ("Trespass to chattels is experiencing a rebirth in modern day policy via Internet advertising."). \textit{See also} Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1230 (N.D. Ill. 2005) ("In recent years, trespass to personal property, which had been largely relegated to a historical note in legal textbooks, has reemerged as a cause of action in Internet advertising an e-mail cases.").
\end{itemize}
A trespass to a chattel may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in possession of another.

One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if, (a) he dispossesses the other of the chattel, or (b) the chattel is impaired as to its condition, quality, or value, or (c) the possessor is deprived of the use of the chattel for a substantial time, or (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.\(^{50}\)

The computer is a user’s personal property. While, the user may have consented to the “free” software that was downloaded, the lawsuit alleged that the user does not consent to downloading the alleged spyware software.\(^{51}\) The condition, quality, and value of the computer can be impaired when the unwanted pop-up advertisements are constantly being displayed onto computer screen, causing disruption to the user’s activity.\(^{52}\)

Plaintiff next alleged that all of the defendants should be liable for unjust enrichment. In Illinois, unjust enrichment occurs when the defendant unjustly retains a benefit to the plaintiff’s detriment, and the retention of that benefit “violates the fundamental principles of justice, equity, and good conscience.”\(^{53}\) Plaintiff alleged that DirectRevenue, aQuantive, and AccuQuote were all unjustly enriched by receiving additional advertising fees and business from the pop-up advertisements that were wrongfully displayed on the plaintiff’s computer.\(^{54}\)

Plaintiff also made further allegations against DirectRevenue alone. Plaintiff alleged that DirectRevenue’s practices had violated Illinois’ Consumer Fraud Act, the computer tampering provisions of the state’s criminal code, and common law negligence standards. Illinois’ Consumer Fraud Act prevents “unfair methods of competition and unfair or deceptive acts or practices, including . . . any practice described in § 2 of the Uniform Deceptive Trade

---

50. Restatement (Second) of Torts, §§ 217, 218 (1965). See also Sotelo, 284 F. Supp. 2d at 1229.
52. Id.
Plaintiff alleged that DirectRevenue’s practices of offering “free” software to computer users without fully disclosing the spyware program that is bundled into the software, and its confusing and misleading installation and removal practices violated § 2 of the Uniform Deceptive Trade Practices Act, and thus the Illinois Consumer Fraud Act. Plaintiff also alleged that DirectRevenue’s actions violated the computer tampering provisions of Illinois’ Criminal Code. Illinois’ Criminal Code provides the following:

(a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer’s owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him: ***

(4) Inserts or attempts to insert a “program” into a computer or computer program knowing or having reason to believe that such “program” contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such “program”

Illinois law allows a plaintiff to pursue a private cause of action against violators of the above provision.

D. Remedies Sought

Plaintiff’s prayer for relief asked the court to award compensatory damages (associated with lost time, use and money spent on programs to remove the software) and injunctive relief to prevent the defendants’ from downloading the spyware software onto computers in such a deceptive manner.

55. 815 ILL. COMP. STAT. 505/2 (2005).
57. 720 ILL. COMP. STAT. 5/16D-3 (2005).
58. Id.
IV. SURVIVING A MOTION TO DISMISS

All of the defendants filed motions to dismiss the plaintiff's complaint, but on August 29, 2005, United States District Court Judge Robert Gettleman rendered a decision that was markedly in the plaintiff's favor, as he allowed a substantial majority of the claims to proceed. The defendants' motions to dismiss focused on jurisdictional arguments and the legal merits of plaintiff's causes of action.

The opinion on defendants' motions to dismiss first discussed the jurisdictional arguments that were made by the defendants. Defendant, DirectRevenue Holdings, first argued that it was merely acting as a holding company for the distributors of the software, and did not have sufficient minimum contacts to subject itself to personal jurisdiction in Illinois as an out of state corporation. The court found that "a holding company that neither transacts business nor contracts to provide a product or services in Illinois is not subject to personal jurisdiction in Illinois," and the claims against DirectRevenue Holdings, LLC were dismissed.

The remaining defendants, however, were either Illinois corporations or had sufficient minimum contacts with the state to be subject to personal jurisdiction in Illinois, and could not make that argument. These remaining defendants instead argued that the court should not have jurisdiction over the case because the litigation should be stayed in favor of arbitration as required by the End User Licensing Agreement. DirectRevenue's licensing agreement has an arbitration clause that requires the parties to submit "any and all disputes, controversies, and claims relating in any way to the Software, this Agreement or the breach thereof" to arbitration in New York, and the Federal Arbitration Act requires courts to enforce valid, written clauses. The defendants' argued that the arbitration clause in the End User Licensing Agreement was valid and enforceable, and as such, the litigation should be stayed in favor of arbitration under the Federal Arbitration Act.

The court disagreed, because the complaint alleged that the End User Licensing Agreement was not even shown to the plaintiff. The
defendants argued that even if the licensing agreement was not viewed by the computer user, that the computer user at least had the opportunity to view it through clicking on a question mark icon that appeared in the right hand corner of the advertisements that were sent through DirectRevenue's software.\(^{65}\)

The argument that the "availability" of the End User Licensing Agreement can render the agreement (and the arbitration clause) enforceable is similar to the arguments that "click wrap" or "shrink wrap" licenses in software packages that are viewed only after the product is purchased are also enforceable.\(^{66}\) However, the court distinguished DirectRevenue's End User Licensing Agreement from such software licensing agreements that were enforced by the Seventh Circuit in the case of ProCD v. Zeidenberg.\(^{67}\) In ProCD v. Zeidenberg, the Seventh Circuit found that a license agreement could be enforced,\(^{68}\) even when not viewed by the purchaser, so long as (a) the plaintiff was given notice of the existence of an agreement prior to purchasing the product, and (b) the plaintiff was afforded an opportunity to return the product if he/she did not agree with the terms of the licensing agreement.\(^{69}\) In Sotelo, the court found that there was not sufficient notice of the existence of an End User Licensing Agreement, and the deception involved in uninstalling the product made it much more difficult for a consumer to "return" the spyware product (as opposed to the software purchased from a store) if he/she disagreed with the terms of the licensing agreement. After finding that the notice of the End User Licensing Agreement did not make this agreement similar to the unseen licensing agreements that were enforced in ProCD, the court found that a triable issue of fact existed, and it denied the defendants' motions to dismiss the case in favor of arbitration.\(^{70}\)

The defendants' also attacked the sufficiency of plaintiff's legal claims, with the most important legal discussion centering on plaintiff's claims against all defendants for trespass to chattels. The court noted that "there is sparse Illinois case law from the last century

\(^{65}\) Id.
\(^{66}\) Id.
\(^{67}\) Id.
\(^{68}\) The Seventh Circuit controls the federal district hearing the Sotelo v. DirectRevenue, LLC case.
\(^{69}\) ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450-53 (7th Cir. 1996); Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1228 (N.D. Ill. 2005).
\(^{70}\) Sotelo, 384 F. Supp. 2d at 1228.
addressing the elements of trespass to personal property,” but the tort “which had largely been relegated to a historical note in legal textbooks has reemerged as a cause of action in Internet advertising and e-mail cases.”

The court’s opinion, which considered the defendants’ arguments for dismissing the trespass to chattels claim, made three important points. First, Judge Gettleman noted that while previous cases establishing a trespass to chattels claim for Internet interference had been brought on behalf of an Internet Service Provider, the distinction between the Internet Service Provider status of the plaintiffs in those cases, and the individual computer user status of Mr. Sotelo and the other class members in the present case was immaterial. “The elements of trespass to personal property—interference and damage—do not hinge on the identity of the plaintiff, and the cause of action may be asserted by an individual computer user who alleges unauthorized electronic contact with his computer system that causes harm.” The harm suffered to the plaintiff’s computer (use of memory and screen pixels), is similar to the harm the court recognized the plaintiff had suffered in CompuServe. The cases that established the use of trespass to chattels for other Internet-related interferences, such as spam or unauthorized web crawlers, did not make a distinction between the status of the plaintiff as an Internet Service Provider in finding that there was damage to the computers. Recognizing that the harm the Internet Service Providers’ computers suffered is similar to the harm the plaintiff’s individual computer has suffered is important, as it allows the individual computer user to bring the claim for damage to his or her own computer.

The second important point that was made in the opinion was that in denying AccuQuote (pop-up advertiser) and aQuantive’s (Internet marketing agency) motions to dismiss, the court recognized that advertisers and agents could also be liable for the damage they were causing to the user’s computer through their alleged

71. Id.
72. Id. at 1230.
73. Id.
74. Id. at 1230-31.
participation in the spyware industry. AccuQuote and aQuantive both argued that they had no control over the displaying of the End User Licensing Agreement, and thus had no intent to unlawfully trespass onto plaintiff’s computer. The court clarified that the advertisers need not “intend” to trespass or violate the law; the plaintiff’s claim was sufficient when it alleged that “AccuQuote and aQuantive, intentionally placed or caused to be placed advertisements through spyware that unlawfully interfered with plaintiff’s use of his computer and Internet connection.” Through recognizing that companies who intentionally work with others who trespass onto computers can be liable, the opinion expanded the scope of defendants to allow plaintiff to more effectively put an end to the unlawful spyware practices.

Finally, the third important point made in the opinion related to the discussion on the damages plaintiff suffered from the pop-up advertisements. Both AccuQuote and aQuantive argued that “plaintiff fail[ed] to allege that they caused actual damage to his property.” Defendants believed there could be no damage because “each individual advertisement can be closed by the computer user as it appears, they cannot cause any actionable injury.” The court looked beyond the damage caused to a computer from just one pop-up advertisement and looked at the damage caused by spyware with a broader perspective as it found that “[defendants’] argument ignores the reality of computer and Internet use, and plaintiff’s allegations that part of the injury is the cumulative harm caused by the volume and frequency of the advertisements.” The harm from DirectRevenue’s software is the excessive number of pop-up advertisements sent out by DirectRevenue in numbers reaching approximately 1.5 billion in one month alone. The high volume of advertisements and the rapid rate at which they continuously pop-up onto the user’s screen cost the computer user lost time and productivity and burden the machine through consuming additional memory and screen display space.

With regards to the remaining counts in the plaintiff’s complaint, the court dismissed plaintiff’s unjust enrichment claim after finding that the defendants did not retain a benefit that plaintiff would

76. Sotelo, 384 F. Supp. 2d at 1231.
77. Id. at 1232.
78. Id.
79. Id.
80. Id. at 1232-33.
81. Id. at 1233.
82. Id.
otherwise be entitled to receive, but allowed the remainder of plaintiff's claims for consumer fraud, negligence, and criminal computer tampering to proceed.  

V. LANDMARK SETTLEMENT REACHED

Just as the *Sotelo v. DirectRevenue, LLC* case was reaching the class certification stage of litigation, the parties reached a settlement agreement that has been characterized as potentially having "powerful implications for the business model of all adware and spyware companies." The injunctive terms were aggressive and have been characterized by BNA as "reforms to ease the burden on consumers." In short, the agreement helps to correct the practices plaintiff alleged were the most misleading and deceptive about the DirectRevenue software.

---

83. Id. at 1233-36.


86. The injunctive terms of the settlement agreement, in their entirety, are as follows:

a. DirectRevenue will not collect any personally identifiable information (name, address, social security number, e-mail address, bank account information, etc.) about computer users. To the extent that DirectRevenue possesses any such data, said data will be destroyed. DirectRevenue shall provide to Class Counsel an affidavit by one of its officers so certifying the destruction and non-existence of such data within fourteen (14) days of the Effective Date of this Agreement.

b. DirectRevenue will assure that, prior to the installation of the Software, computer users are (a) provided with DirectRevenue's End User License Agreement ("EULA"), and (b) given two choices, of equal prominence within the modal box or landing page, to the effect of:

   "I have read and accept the agreement" or
   "I do not accept the terms of the agreement"

The "accept" option will not be a default option. If the user selects the "I do not accept" choice, the Software will not be installed.

c. In addition to providing computer operators with its EULA, DirectRevenue will also disclose, separate and apart from the EULA, that: (1) users will receive advertisements while online, along with a brief description of the types of ads that will be displayed; (2) DirectRevenue will collect information about web sites visited by users; (3) users may receive ads with adult content if and while they are visiting websites with adult content; and (4) the Software will be included in their installation of the ad-supported software. This disclosure will be independently displayed within the modal box containing the "I have read and accept" and "I do not accept" choices described above. The additional disclosures shall appear above the choices described in subparagraph b, above, but will end no more than one inch away from those choices.
d. DirectRevenue will not install Software via ActiveX installations, security exploits, or by any other method that does not require users' affirmative consent.

e. In DirectRevenue's EULA, DirectRevenue will disclose the fact that the Software serves pop-up ads based on websites visited by the user, and that DirectRevenue collects non-personally identifiable information, in order to serve those ads. The EULA will explain DirectRevenue's use of the non-personally identifiable information. The EULA will also notify users as to how the Software can be uninstalled, and will provide information on how to access DirectRevenue's website and customer support.

f. Without charge, DirectRevenue will provide help to consumers in removing the Software via e-mail. In addition, DirectRevenue will provide a toll free telephone number that will allow consumers to call and receive a recorded message that includes: (1) detailed instructions about how to remove the Software, and (2) information directing users to locations on the Internet to learn more information about how to remove the Software.

g. In new distribution contracts, DirectRevenue will require distributors to abide by the policies represented in this settlement. DirectRevenue will closely police its distributors. If DirectRevenue learns that a distributor is violating these terms, DirectRevenue will take appropriate action based on the circumstances of the violation, potentially including termination of the distributor.

h. Distributors will not be permitted to use sub-distributors unless those entities are bound by contract to adhere to the policies represented herein.

i. DirectRevenue will not distribute the Software via websites targeted primarily at children. The EULA will include a disclosure that the Software should only be installed by users 18 years of age and older, and instructions (or a reference link to such instructions) on how to manage the user's operating system to minimize the possibility that children will be served with ads by the Software. DirectRevenue will disclose to Net Nanny (and similar services) the IP address of any server sending adult content ads through the Software.

j. DirectRevenue will not use the word "free" in banner ads describing the underlying program (i.e., the screen saver or video game) unless the ad also discloses that the program is ad-supported.

k. When the Software displays a pop-up ad, the "X" button on the title bar of the ad window (used to close the ad window) will not appear off-screen, unless this effect is caused by a technical issue without DirectRevenue's knowledge or beyond DirectRevenue's control.

l. All DirectRevenue ads will include a "?" button on the title bar, or a text link indicating that further information is available, which displays information about the Software when clicked. This information will include (1) an explanation of why the user is receiving the ad; (2) the identity of the consumer application the user downloaded with the Software (when and to the extent this is technically feasible); and (3) an instruction that, if the user so desires, the user can uninstall the Software using the Windows "Add/Remove Programs" function.

m. The Software will not display adult content ads unless the user is viewing adult websites. DirectRevenue will disclose to Net Nanny (and similar services) the IP address of any server sending adult content ads through the Software.

n. The Software will be listed in the Windows "Add/Remove Programs" list under the exact same name used in branding the ads. DirectRevenue will make removal of the Software easy.

o. DirectRevenue will not modify security settings on users' computers.

p. DirectRevenue will not reinstall its Software once a user has uninstalled it through the Windows "Add/Remove Programs" function, unless the user later opts to download
The terms of the agreement require DirectRevenue to take certain steps that will help to ensure consumers are fully informed about the character of the software, before such software is downloaded onto a computer. Prior to installing its software onto a computer, DirectRevenue must notify users of the EULA; provide additional explanations and descriptions about the software that will be downloaded; and provide users with clear options to either accept or reject the product after reviewing these terms and descriptions.

Once the software is downloaded, the agreement also requires DirectRevenue to take measures that will ease the confusion and deception that plaintiff alleged previously surrounded the uninstallation process. DirectRevenue’s pop-up advertisements must all now contain a “question mark” icon that, once clicked, will direct users to information that explains why the user is receiving the pop-up advertisement and instructions on how the program can be uninstalled. DirectRevenue is also obligated to provide help to users who wish to uninstall the software. This help will be available through e-mail or a toll-free telephone line that will provide instructions and information on how to remove the software. DirectRevenue must also take measures, such as limiting the number of times it changes its corporate name and using the same corporate

and install another bundled application and the installation proceeds in accordance with the terms herein.

q. DirectRevenue will not delete other software on the user’s computer other than any underlying program (e.g., screensaver) that was bundled with the Software upon the user’s removal of the Software.

r. DirectRevenue will not materially modify the Software’s functionality without providing the user with notice and an opportunity to uninstall the Software.

s. DirectRevenue will agree to limit its advertisements to a network average of 10 or less per computer per 24-hour period.

t. DirectRevenue agrees that its removal instructions shall continue to be posted in a form in substantial conformity with that currently found at: http://www.bestoffersnetworks.com/uninstall/.

u. Upon request by e-mail identifying the user seeking assistance as visually impaired, DirectRevenue will personally assist (through live telephone support) any visually impaired person in removing the Software.

v. DirectRevenue will limit its number of name changes used on its advertisements (i.e., “Best Offers”) to once per two years.

w. DirectRevenue will agree to purchase sponsored links, if Google is willing to sell such sponsored links, that provide links to help consumers remove DirectRevenue software. At a minimum, DirectRevenue will agree to purchase links, if Google is willing to sell such sponsored links, for “Best Offers” and “Best Offers removal”. By clicking on the sponsored link, the user will be taken to an Internet page with instructions on how to remove the Software. Should DirectRevenue change the name of its software, it will purchase sponsored links with the new name of the Software referenced.
name on its software programs and advertisements, to help consumers to easily identify the company once the software has been installed on the user’s computer.

The settlement agreement provides sweeping relief to help to curb the practices that were overwhelming users’ computers with unwanted pop-up advertisements. Through the settlement, DirectRevenue has agreed to limit the number of pop-up advertisements it will send out (no more than an average of ten on a network average per computer during a 24-hour period), and change the practices that allegedly frustrated and deceived consumers during the installation and uninstallation process. These changes will help to protect consumers through informing them about the software that is being downloaded onto their computers and providing clearer methods consumers can use to uninstall the software. In addition, pursuant to the settlement agreement, Illinois residents are still permitted to individually seek monetary relief against DirectRevenue for damage that was caused to their computers.

VI. DISTINGUISHING SOTELO V. DIRECTREVENUE FROM PREVIOUS SPYWARE CASES

Pop-up advertisements and the spyware software industry have previously been attacked in other litigation. These previous cases have been met with limited success; however, the distinctions in Sotelo v. DirectRevenue LLC’s complaint and legal claims demonstrate that Sotelo had stronger legal claims to allow it to yield a more successful result in the end.

Previous cases attacking pop-up advertisements have typically been brought on behalf of companies who are disenchanted with the idea that when a consumer searches and views their web page, the spyware software will track the user’s Internet activity and send pop-up advertisements from the companies’ competitors to the user’s computer screen. The pop-up advertisements are causing damage to


89. See Gator.com v. L.L. Bean, Inc., 398 F.3d 1125, 1127 (9th Cir. 2005); 1-800 Contacts, Inc. v. WhenU.com, Inc., 414 F.3d 400, 404-05 (2d Cir. 2005); U-Haul Int’l v.
the computer and not the web page, so actions for trespass to chattels have not been available to these plaintiffs who only have a possessory interest in the web page and not the user's own personal computer. These companies have instead argued that the pop-ups that are appearing over their web page constitute copyright and trademark violations. However, because the pop-ups do not copy or use the copyrighted or trademarked material, or alter the contents of the web page, courts have found that the claims for the copyright violations cannot be established.90

The allegations in Sotelo v. DirectRevenue, LLC can be distinguished from these cases, as the plaintiff here does have standing to pursue a trespass to chattel claim. As previously discussed, trespass to chattels has a solid legal foundation. courts have accepted that this tort can be a strong cause of action to against Internet-related interferences.91 The plaintiff's complaint has established a strong legal foundation by demonstrating the specific damage that results from the pop-ups that are distributed through DirectRevenue's spyware software.92 The plaintiff's legal standing on the trespass to chattels claim and specific damage allegations demonstrate that Sotelo v. DirectRevenue, LLC can be distinguished from other pop-up advertisement cases and will help to set a strong legal precedent for future litigation.93


92. Contra DirectTV, Inc. v. Chin, No. SA-03-CA-0660-RF, 2003 WL 22102144 (W.D. Tex. Aug. 26, 2003) (dismissing a trespass to chattels claim against a pop-up advertiser when plaintiff did not allege any specific type of damage, but merely "[made] a general claim that, 'on more than one occasion,' Plaintiff's 'pop up' ads have appeared on his computer").

93. See generally Slutsky, supra note 88 (noting the difference between the previous cases and Sotelo).
CONCLUSION

Sotelo v. DirectRevenue, LLC will have a considerable impact in the area of Internet-related case law and on the spyware industry. The impact of this decision has already been realized, as other lawsuits have subsequently been filed. The court’s opinion denying defendants’ motion to dismiss is significant. The opinion recognizes that a claim for trespass to chattels can be used to attack unauthorized pop-up advertisements that appear on one’s computer. The opinion also establishes that all computer users—not just Internet Service Providers—can pursue claims for damage caused to their individual computers, and recognizes that all parties involved, including advertisers and agents, can be liable for trespass to chattels if the computer itself is damaged from the repeated number of pop-ups received. The settlement that was reached will also help to correct the allegedly deceptive practices associated with the software so that consumers will be protected through being more informed about the character of the software before it is downloaded onto a computer.
