

FILED
DISTRICT COURT
MAY 19 PM 5:40
THIRD JUDICIAL DISTRICT
SALT LAKE COUNTY

Blake D. Miller (4090)
Paxton R. Guymon (8188)
Joel T. Zenger (8926)
MILLER MAGLEBY & GUYMON, P.C.
170 South Main Street, Suite 350
Salt Lake City, Utah 84101
Telephone: (801) 363-5600
Facsimile: (801) 363-5601
Special Assistant Attorneys General

BY _____
DEPUTY CLERK

Mark Shurtleff (4666)
Philip C. Pugsley (2661)
UTAH ATTORNEY GENERAL'S OFFICE
160 East 300 South
Suite 500
Post Office Box 140811
Salt Lake City, UT 84114-0811
Telephone: (801) 366-0245
Facsimile: (801) 366-0352

Attorneys for Defendants

IN THE THIRD JUDICIAL DISTRICT COURT
SALT LAKE COUNTY, STATE OF UTAH

<p>WHENU.COM, INC. a Delaware corporation,</p> <p style="text-align: center;">Plaintiff,</p> <p style="text-align: center;">vs.</p> <p>THE STATE OF UTAH, a body politic, OLENE S. WALKER, in her official capacity as Governor of Utah., and MARK SHURTLEFF in his official capacity as Utah Attorney General,</p> <p style="text-align: center;">Defendants.</p>	<p>MEMORANDUM IN OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION</p> <p>Civil No. 040907578</p> <p>Honorable Joseph C. Fratto</p>
--	--

INTRODUCTION

The use of spyware has exploded. It is estimated that over ninety percent of all personal computers with Internet broadband connections in the United States are infected with spyware.¹

Spyware has eclipsed viruses as the major threat to computers. One reason for this is the significant economic incentives for the continued development and dissemination of spyware. Although viruses are often the product of individuals with little to no economic incentive, spyware is the product of well-financed companies with substantial profit motivations.

Spyware is software that is installed on a computer without the user's informed consent. Such software then monitors certain aspects of the computer's use. Spyware not only threatens a computer user's personal information, but often degrades the infected computer's performance. Difficulties caused by spyware are now the single largest reason for complaints to computer manufactures and internet service providers. In addition to the substantial harm to computer users, spyware also causes damages to Utah companies who spend millions of dollars on their websites, only to find their sites the targets of superimposed competing advertisements generated by spyware. Utah's Spyware Control Act, codified at Utah Code Ann. 13-39-101, *et. seq* (the "Spyware Act" or "Act") addresses these legitimate state concerns.

STATEMENT OF FACTS

Spyware can take many forms. The essence of spyware, however, is software that is installed without the computer users' knowledge or informed consent, that monitors the computer's usage, sends information about the computer's usage to a remote computer or

¹ See Surmacz, *Most Computers with Broadband Access Vulnerable to Spyware*, <http://www.csoonline.com/metrics/viewmetric.cfm?id=562> (June 19, 2003).

interferes with the use of a website. Spyware can be keyloggers, chat monitors, screen recorders, program loggers, email recorders, password records, modem hijackers, screen recorders, trojans, webbugs, or adservers. The essence of such programs is that they secretly record computer usage and transmit that information to another computer or server. In the case of adservers, such software monitors computer activity to determine areas in which the computer user shows an interest in order to effectuate targeted marketing. For example, if an individual uses his or her computer to investigate funeral options, the software displays unsolicited funeral related advertisements on the person's computer screen.

Some spyware targets websites of specific companies. Such spyware detects when a user attempts to view a pre-targeted website and then immediately causes another advertisement, not requested by the user, to be placed over the targeted site. These advertisements are known as "pop-up" advertisements because they automatically appear in a separate window on the user's computer monitor over the intended viewing area without any action by the user. The user must then act affirmatively to move or close the pop-up advertisement in order to view the screen of the targeted website. Pop-up advertisements are notably offensive and rank among the most annoying intrusions in consumer's lives. One market research firm found that pop-up advertisements ranked second only to telemarketing as less desirable advertising, including junk mail. Julia Angwin & Mylene Magnalindan, *America Online Will Put Down Its Pop-Up Ads*, Wall St. J., Oct. 16, 2002, at B4.

Such pop-up advertisements are designed to lure the user away from the targeted site. Therefore, if the computer user clicks on the pop-up advertisement, he or she is then redirected to

a competitor's website. For example, if a computer user attempts to access an airline webpage which is targeted by installed spyware, the spyware will detect that access and then cause a pop-up advertisement of another travel company to appear over the targeted webpage. If the user clicks on the pop-up, the user's web browser is then directed to the other travel site. For example, OnAd Solutions uses the following demonstrated in marketing its targeting software capabilities to companies interested in having their advertisements pop-over a competitor's website. In this example, when a computer attempts to view the ETrade website, the pop-up advertisement for ETrade's competitor, Datek appears:

The image shows a screenshot of the OnAd Solutions website. At the top left, the OnAd Solutions logo is displayed with the tagline "THE HOME OF 'SMART TRAFFIC'". Below the logo is a navigation menu with links for HOME, SERVICES, ABOUT US, and CONTACT US. The main content area features a "Live Campaign Snap Shot" section. This section includes a screenshot of the ETrade.com website with a Datek advertisement overlaid. The advertisement is titled "Our Difference" and lists several features. To the right of the screenshot, there is a text box that reads: "When ETrade.com is visited, a 585x261 ad is displayed showing Datek's homepage." Below this text box, there is a "Next" button. The overall layout is clean and professional, with a focus on demonstrating the targeting capabilities of the software.

ON AD SOLUTIONS
THE HOME OF "SMART TRAFFIC"

HOME SERVICES ABOUT US CONTACT US

E*TRADE

DATEK

Our Difference

When ETrade.com is visited, a 585x261 ad is displayed showing Datek's homepage.

Extended Hours Trading

Live Campaign Snap Shot

When users browse the web, On Ad Solutions will identify those viewers interested in your company and provide an instant targeted offer.

As an example, when a user visits Etrade.com online, we can deliver an "Instant Message" from Datek.com. This type of Real-time targeting delivers CTR percentages of up to 14%, almost 30 times that of other internet advertising.

Next

See, <http://www.onadsolutions.com/demo1.html>.

All too often, the pop-up advertisement of the competitor does not clearly indicate that it is not part of the website selected by the consumer. Substantial research has confirmed that consumers are typically misled into a false perception that the pop-up advertisement was generated by the targeted website and that pop-up advertisements are not well received by computer users. As a result, not only are companies unable to control how their website appears on computers infected with such spyware, but the targeted use of pop-up advertisements leads to substantial consumer confusion.

Pop-up advertisements generated by spyware are not generated by the targeted website. Rather, they are sent by the spyware company to the user's computer in response to detection that the user was attempted to access a targeted website. These targeted spyware pop-ups are distinguishable from pop-ups which are created by the website owner. In the latter pop-ups, the advertisements become part of the website that the website operator designed, and the website owner controls how the pop-up advertisement interrelates with the website.

Spyware is, by definition, unwanted by the computer user (or at the least not chosen with informed consent). Also typical is the fact that such software is installed on computers without the user's knowledge. This is done in a variety of ways. It is often installed on a "Trojan Horse" model. In such cases, spyware is hidden inside software bait – essentially software advertised as "free" – which consumers are enticed to download. The entire purpose of the "free application" is to act as a host that consumers will want to download. When the "free application" is downloaded, the spyware also comes along and installs itself on the computer. In addition,

spyware can become installed as an unrequested "add-on" to third-party programs. Spyware can even be downloaded by other spyware already infecting a computer.

Spyware can also be installed unknowingly as a computer browses an unrelated website. This process is termed "drive-by downloads." Under this method of installation, when users visit certain web pages, those pages cause the user's computer to download and install spyware. Depending on the configuration of the particular computer, drive-by installations may cause the display of a single pop-up message box, which may or may not offer a link to a license agreement, or may not display any message box at all. The appearance of a dialog message box suggests, implicitly or explicitly, that the user has to click yes in order to properly view the website. What the user gets, however, is spyware.

A critical characteristic of spyware is software installed without the user's informed consent. Many of such programs install themselves without displaying a license agreement. Other license agreements are presented in a time or manner which discourages the consumer from reading and understanding what will happen to their computers as a result of clicking the "yes" button. Since the spyware installation is essentially a byproduct of some other activity that the computer user actually wants to accomplish, e.g., downloading other software or viewing a website, many users are unaware of how spyware even came to be on their computers.

Spyware typically survives by remaining hidden. To do so, it runs in "stealth mode." Such software is specifically designed to be kept hidden from the computer's user. Spyware is typically not visible in the task list or in the standard startup areas. Once found (often due an investigation into degraded computer performance), the vast majority of users try to remove the

software from their computers. Such removal, however, is often difficult to accomplish. Even if the particularly spyware is listed on the Add/Remove Programs dialog in Windows, installation will typically leave some components behind. To effectively remove the software, the computer user will often have to edit the Windows registry or use third party removal software.

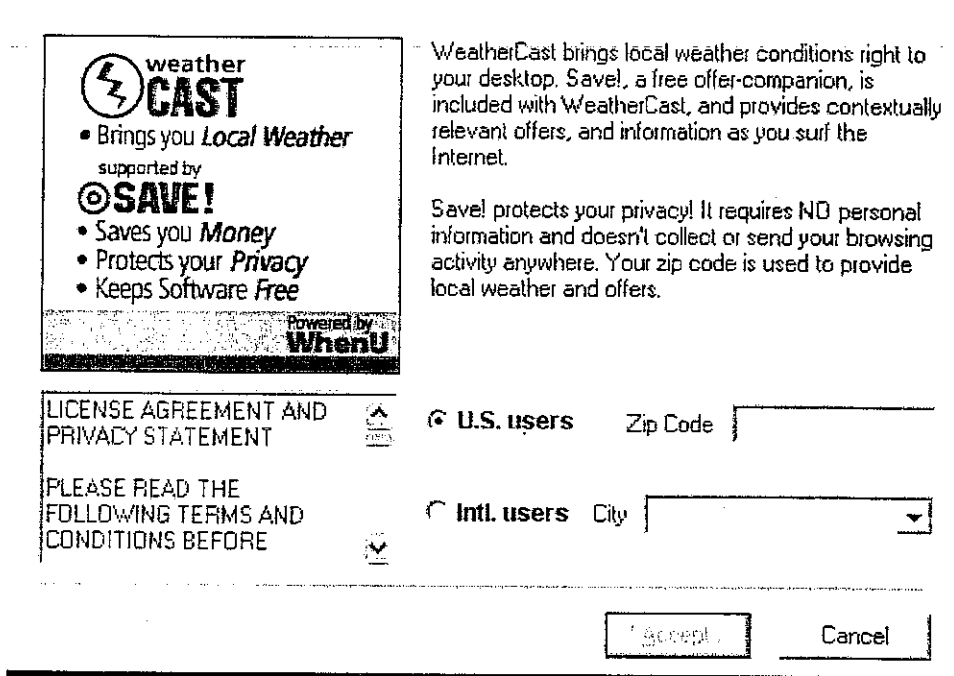
Upon installation, spyware uses that computer's resources and bandwidth to monitor the user's computer activities and relay information. Spyware uses the computer's central processing unit, memory and other resources, together with the consumer's purchased bandwidth, in order to connect to the Internet and upload whatever information the software is designed to convey and to download advertisements. Although spyware distributors are quick to argue that their software is as gentle on computer resources as it is highly desired by consumers, spyware typically significantly decreases computer performance, slows webpage viewing, changes the appearance of websites, creates pop-up advertisements, modifies computer settings and even creates substantial security risks, such as creating "holes" in firewalls and other computer protections.²

Although WhenU complains that it is being unfairly targeted by the Spyware Act, the Act actually is designed to combat all forms of spyware.³ Since WhenU is the plaintiff in this matter, however, a description of WhenU's software is appropriate. WhenU software is bundled with other "free" software applications, such that when the user downloads the free application, the

² The comparison of resource use to consumer desirability might be apt, since the vast majority of consumers attempt to disinfect their computers once spyware is discovered.

³ WhenU goes to great length to argue that it really isn't spyware at all, since WhenU claims that its software is voluntarily downloaded by consumers after informed consent. WhenU doesn't seem to complain that Utah doesn't properly have an interest in combating true spyware – where such software is installed without informed consent.

WhenU adware is also installed. One of WhenU's contextual based targeting software is bundled with a "free application" entitled "WeatherCast". When WeatherCast is installed, the following box appears:



The License Agreement and Privacy Statement is viewable in full only by the user clicking on the down-arrow key approximately 300 times.

WhenU has utilized the foregoing Trojan Horse model of distribution as well as the drive-by model. When users receive WhenU software via drive-by download, they may or may not consent to WhenU's license agreements. Users may never even see WhenU's license agreement, because WhenU's drive-by installer does not show the license to users, even in part. Instead, the installer merely offers a link to the license – which license might not be viewable. See, *Declaration of Benjamin G. Edelman*. According to a survey conducted by PC Pitstop, a

website that provides technical support for computer problems, 87% of users with WhenU installed on their systems didn't know it. See, <http://www.pcpitstop.com/spycheck/whenu.asp>.

After installation, the WhenU software monitors the computer activities, looking for attempts to access targeted websites. When a computer WhenU software attempts to access a targeted website, WhenU causes a pop-up advertisement to appear at approximately the same time as the targeted website. The WhenU pop-up advertisement typically covers portions of the targeted websites and is designed to lure the user away from the targeted website. WhenU does not obtain permission from the targeted website owner and even directs pop-up advertisements to website that do not allow advertising.

Typically, WhenU's pop-up advertisements are from competitors trying to lure customers from targeted sites. For example, if a computer infected with the WhenU software attempts to view a travel site, WhenU will cover the site with an advertisement for a competing travel site with a link directing the browser to that competing site. If a computer attempts to browse a car rental site, a competitor's advertisement is shown. WhenU's euphemism for this business model is "contextual marketing." In plain English, it means that WhenU detects that a computer is attempting to access a targeted website, it intercepts that effort and displays a competing ad over the top of the targeted website.

WhenU is hardly a unique company. It is, rather, one of many companies who entice consumers to download their software with "free applications" in order to sell to its advertising customers the ability to cause their advertisement to appear over certain targeted websites. Other companies who offer similar targeted advertisements include Claria (formerly known as Gator),

eZula, BDE, BargainBuddy, Bonsai Buddy, and TopText, among many others. *See, e.g.*, James R. Hagerty & Dennis K. Berman, *New Battleground in Web Privacy War: Ads That Snoop*, Wall St. J., Aug. 27, 2003. These companies share the business model of selling aggressive “guerrilla marketing tactics” to their advertising customers. Neal S. Greenfield, *“Adware,” “Spyware,” and “Scumware” Plague Advertisers and Internet Users: Is It Illegal?* Metro. Corp. Couns., July 2002, WL 7/02 METCC 12. Although these targeted advertising companies almost always characterize their software as consumer-friendly, third party studies uniformly find that such software is not desired by consumers.⁴ In fact, many consider such activities to be unethical, unscrupulous and illegal. *Id.*

Computer users in Utah are greatly affected by spyware. Spyware degrades computer performance, slows Internet connections, monitors computer activities, and creates serious security risks. Utah companies also suffer as a result of spyware targeted pop-up advertisements. Utah companies, who spend millions of dollars on their website presences and storefronts, have this investment marred by the graffiti of competitors’ spyware generated pop-up advertisements.

The Spyware Act is designed to protect against these harms to Utah consumers and businesses. Section 13-39-102(4) defines “spyware” as software residing on a computer that is installed **without the user’s informed consent** that:

⁴ WhenU asserts that millions of consumers have elected to download their adware “in order to obtain the money-saving offers it provides.” (WhenU memorandum at 1). If that were the consumer’s principal motivation, one wonders why the adware is distributed with free software bait. If WhenU is correct, consumers would simply seek out and install the adware as a stand alone application. WhenU’s argument also ignores the fact that millions of consumers try to remove the WhenU software from their computers after installation. (WhenU memorandum at 6; “tens of millions of computer users” have uninstalled the WhenU software). In actuality, WhenU’s software is approximately as popular to consumers as telemarketing cold calls.

1. Monitors the computer's usage;
2. Sends information about the computer's usage to a remote computer; or
3. Displays or causes to be displayed an advertisement in response to the computer's usage if the advertisement:
 - a. Does not clearly identify the entity responsible for delivering the advertisement;
 - b. Uses a registered trademark as a trigger for the advertisement;
 - c. Uses a triggering mechanism to deliver the advertisement based on the monitored Internet usage; or
 - d. Uses a context based triggering mechanism to display the advertisement obscuring the website intended to be viewed.

The Spyware Act has essentially two prohibitions. First, a person may not install or cause to be installed spyware on another's computer without the user's informed consent. Second, a person may not use a context based triggering mechanism to display an advertisement over a targeted website. Although WhenU claims to never install its software without the user's informed consent, it challenges both aspects of the Spyware Act.

ARGUMENT

I. WHENU IS NOT LIKELY TO PREVAIL ON THE MERITS OF THE UNDERLYING CLAIMS.

WhenU challenges the Spyware Act on several grounds: (1) the Act violates the Commerce Clause of the United States Constitution; (2) the Act violates the First Amendment of the United States Constitution; (3) the Act fails to have uniform application as required under the Utah Constitution; and (4) the Act is preempted by the Federal Copyright law. WhenU is not likely to prevail on the merits of any of these arguments.

A. The Spyware Act Does Not Violate The Commerce Clause.

Challenges to legislation under the dormant commerce clause typically follow a two-tiered analysis. First, the Court considers whether the statute is facially discriminatory. If the statute discriminates on its face by giving protection to in-state interests at the expense of out-of-state interests, in order to survive the law must promote a compelling state interest. *See, e.g., City of Philadelphia v. New Jersey*, 437 U.S. 617, 624 (1978) (“[W]here simple economic protectionism is effected by state legislation, a virtually *per se* rule of invalidity has been erected. . . . The clearest example of such legislation is a law that overtly blocks the flow of interstate commerce at a State’s borders.”).

Where the statute is not clearly protectionist on its face, the Court then employs a balancing test:

Where the statute regulates evenhandedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits. . . . If a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.

Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970). Essentially, the state’s interest in promulgating the legislation is weighed against the burden the legislation may impose on interstate commerce.⁵ Only if the burdens imposed on interstate commerce are “clearly

⁵ WhenU also argues that the Spyware Act should be judged according to two other independent tests, i.e, whether the law has extraterritorial effects and whether it subjects interstate commerce to inconsistent state regulation. (WhenU memo at 19). This “unsettled and poorly understood” analysis is actually appropriately regarding as part of the *Pike* balancing test. *See, e.g., Goldsmith & Sykes, The Internet and the Dormant Commerce Clause*, 110 Yale L. J. 785, 789 (2001).

excessive” in relation to the putative local benefits, will the statute be deemed unconstitutional.

Id.

Under the first analysis, the Spyware Act is clearly not facially discriminatory. A statute discriminates against interstate commerce when it provides for “differential treatment of in-state and out-of-state economic interests that benefits the former and burdens the latter.” *Hughes v. Oklahoma*, 441 U.S. 322, 325-26 (1979). Merely because “the burden of a state regulation falls on some interstate companies does not, by itself, establish a claim of discrimination against interstate commerce.” *Exxon Corp. v. Maryland*, 437 U.S. 117 (1978). Absent a facially discriminatory purpose, a law is discriminatory when it provides for differential treatment of similarly situated entities based upon their contacts with the State or has the effect of providing a competitive advantage to in-state interests vis-à-vis similarly situated out-of-state interests.

Although, similar to the vast majority of other legislation,⁶ the Act does not specifically specify a Utah nexus, it is clear that the purpose of the act is twofold: (1) to prohibit the downloading of spyware on Utah computers, without the informed consent of the user and (2) the improper use of targeted pop-up advertisements on Utah businesses. *See, Affidavit of Stephen H. Urquhart*. When faced with a constitutional challenge, Utah Courts afford legislation a presumption of validity and resolve doubts in favor of constitutionality. *See, e.g., State v. Lopes*, 1999 UT 24, 980 P.2d 191. The Spyware Act applies to **all** persons who download spyware on Utah computers without informed consent. WhenU is not discriminated against due to its contacts, or lack of contacts, with Utah. Rather, it is not WhenU’s contacts with the state, but its

⁶ *See, e.g.,* Utah Code Ann. §76-6-703 (computer crimes and penalties); Utah Code Ann. §76-9-402 & 403 (privacy violation and communication abuse).

offending conduct that is applicable. The Act places no additional burdens on out-of-state persons than it does on in-state citizens. *Exxon Corp.*, 437 U.S. at 126. The Act is totally devoid of any reference which makes it discriminatory to non-Utah citizens.

Therefore, the only issue is whether, under the *Pike* balancing test, the burden imposed on commerce is clearly excessive in relation to the local benefits of the Spyware Act. *Pike* at 142. The party challenging the law bears the burden of establishing that such commerce burden is clearly excessive. *State v. Heckel*, 24 P.3d 404 (Wash. 2001) (party challenging law as unconstitutional has burden of proving it unconstitutional beyond a reasonable doubt). This, WhenU cannot do.

B. Valid State Interests are Promoted by the Spyware Act.

It cannot be reasonably disputed that Utah has an interest in protecting its citizens from the unwanted and undesired surreptitious downloading of spyware onto their computers. Similarly, it cannot be reasonably disputed that Utah has an interest in protecting its businesses from targeted pop-up advertisements that unfairly free-loads on their intellectual property and degrades their website investments. Both interests are valid State interests.

The Supreme Court has long regularly recognized that states may properly pass legislation affecting the health, safety and general welfare of their citizens even where such legislation affects interstate commerce. *Willson v. Black-Bird Creek Marsh, Co.*, 27 U.S. 245 (1829); *New York v. Miln*, 36 U.S. 102 (1837) (“[I]t is not only the right, but the bounden and solemn duty of a state, to advance the safety, happiness and prosperity of its people, and to provide for its general welfare, by any and every act of legislation which it may deem to be

conducive to those ends.”). Utah certainly has an interest in passing consumer protection laws or unfair competition or business practices laws. The Spyware Act falls within these categories. In addition, Utah has a very real interest in protecting the interests of its citizens and businesses from manipulative and improper practices – even if accomplished in part via the Internet. The mere fact that the Internet is involved does not make these state interests vanish.

Case law supports the proposition that states have the ability to protect their citizens from improper business activities, even if conducted through the Internet. For example, in *Ford Motor Co. v. Texas Dept. of Trans.*, 264 F.3d 493 (5th Cir. 2001), the court upheld a Texas motor vehicle statute as it applied to Ford’s sales of vehicles through an Internet website. As WhenU does in this case, Ford argued that the application of the Texas statute violated the dormant commerce clause. After rejecting the claim that the statute discriminated against out-of-state interests, the Court analyzed the statute under the *Pike* balancing test.

Similar to WhenU in this case, Ford argued that its Internet showroom offered great benefits to consumers. (“WhenU provides a valuable service to Consumers,” WhenU Memo at 3). Since the alleged benefits of the activity of the challenging party are simply not relevant to the *Pike* balancing test, the Court properly ignored such statements:

As evidence of the burden on commerce caused by § 5.02C(c), Ford extols the benefits of the Showroom to consumers, Texas automobile dealers, and Ford itself. The district court correctly ignored these alleged benefits, the elimination of which is not a constitutional burden on commerce. These arguments relate to the economic efficacy of the statute and are misdirected to this Court. *Exxon*, 437 U.S. at 128, 98 S.Ct. 2207 (“It may be true that the consuming public will be injured . . . but . . . that argument relates to the wisdom of the statute, not its burden on commerce.”).

Id. at 503. Instead, Ford was required to establish that the legislation imposed an impermissible burden on interstate commerce. This, Ford was unable to do.

Ford asserted, as does WhenU, that the Internet requires national uniformity, which need outweighs Texas' interest in regulating the activity in question. Since the legislation prohibited conduct (selling vehicles without a license) and not the Internet itself, the Court had no difficulty holding that this concern was misplaced. The Court noted that bad conduct cannot be given amnesty simply because it is conducted via the Internet. According to the Court, "corporations or individuals [should not be allowed to] circumvent otherwise constitutional state laws and regulations simply by connecting the transaction to the internet." *Id.* at 505.

Similarly, the Spyware Act does not attempt to regulate the Internet, but bad conduct that may be accomplished, in part, by the Internet. Simply because WhenU, and other spyware distributors, choose to use the Internet, does not give them carte blanche exception from state regulation. If WhenU's arguments are taken to their logical conclusion, states would have no ability to regulate any activities conducted, in part, through or by the Internet. Fraud, securities violations, gambling, libel, computer crimes, unfair competition, etc, would all be free from state regulation as long as the perpetrator was smart enough to utilize the Internet. Clearly, this is in error.

C. The Spyware Act Imposes Minimal Burdens On Interstate Commerce.

WhenU attempts to characterize the Spyware Act as a blatant attempt to regulate the Internet. In fact, according to WhenU, the Act would have the effect of no less than the denegation of the entire software industry and the global Internet: "If the act were to go into

effect, it would impose substantial burdens on Internet commerce throughout the United States and the world and would retard the growth of the software industry and Internet commerce.” (WhenU memorandum at 20).

An impartial and fair reading of the Act reveals no such ambitious attempt to regulate the software industry or the Internet. Rather, the Spyware Act simply prohibits improper conduct, such as the surreptitious installation of spyware on computers in Utah and/or the targeting of websites by pop-up advertisements through software that intercepts a person’s attempt to view a specific website. Such conduct has been held improper by a number of courts. *See, e.g., Washingtonpost.Newsweek Interactive Co. v. Gator Corp.*, No. 02-909-A, 2002 WL 31356645 (E.D. Va. 2002) (Gator enjoined from causing its pop-up advertisements to be displayed on the plaintiff’s websites or infringing the Plaintiff’s trademarks on grounds the use of such pop-ups violated plaintiff’s intellectual property rights).⁷ Simply because improper conduct is done by way of the Internet does not provide amnesty to the wrongdoer. *See, e.g., Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999) (issuing preliminary injunction that, among other things, required two critics of the Mormon Church to remove from their website the addresses of third-party websites that the critics knew, or had reason to know, contained copies of copyrighted work).

WhenU relies on the increasingly criticized opinion of *American Library Ass’n v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997), for the bold proposition that activities occurring on the Internet should be, axiomatically, exempt from state regulation. *See, e.g., The Dormant*

⁷ The parties reached a settlement in February, 2003.

Commerce Clause and the Internet, 17 Harv. J.L. & Tech. 296 (Fall 2003) ([the *Pataki*] analysis has been rejected by other courts evaluating state laws regulating the Internet, and wisely so); William Lee Biddle, *State Regulation of the Internet: Where does the Balance of Federalist Power Lie?* 37 Cal. W. L. Rev. 161 (Fall 2000) (*Pataki* has clearly gone too far in declaring that courts have held an area of interstate commerce off limits to state regulation). The better reasoned cases do not depend on a sweeping characterization such as relied on by *Pataki*, but rely on a more careful analysis of the specific type of regulation and the state interest involved in the particular case.

A number of courts, utilizing the more reasoned approach, have held that laws that have some impact on conduct that occurs or is facilitated by the Internet are not barred by the commerce clause. For example, in *Hatch v. Superior Court*, 80 Cal. App. 4th 170 (4th Dist. 2000), the Court upheld a criminal statute imposing liability for sending harmful or indecent material to a child. In this case, the plaintiff used the Internet to send indecent material to a woman in California posing as two 13 year old girls. The Court rejected the plaintiff's challenge to the law under the Commerce Clause. The Court found that California had a proper interest in protecting minors from the subject harm. The Court rejected the claim, advanced in *Pitaki*, that states were prohibited from regulating conduct if such improper conduct occurred through the use of the Internet:

While it may be true that Internet communications routinely pass along interstate lines, we do not believe this general proposition can be employed, as suggested by *Hatch*, to insulate pedophiles from prosecution simply *by reason of* their usage of modern technology. Such a view of what our Constitution requires is, in our opinion, completely inappropriate.

Id. at 471 (emphasis in original). See, also, *People v. Hsu*, 82 Cal. App. 4th 976 (1st Dist. 2000) (after sending suggestive photos to a minor in California by way of the Internet, plaintiff's challenge under commerce clause rejected); *People v. Foley*, 731 N.E.2d 123 (N.Y. 2000), *cert. denied*, 531 U.S. 875 (2000) (challenge to law under commerce clause rejected where plaintiff charged with disseminating indecent material to a New York resident via the Internet).

Cases upholding state laws which impact Internet conduct against commerce clause challenges are not limited to pornography cases. For example, in *People v. Lipsitz*, 663 N.Y.S.2d 468 (N.Y. Sup. Ct. 1997), the court upheld a New York consumer protection statute as to a business that engaged in consumer fraud through e-mail solicitations. As stated by the Court, "there is no compelling reason to find that local legal officials must take a "hands off" approach just because a crook or con artist is technologically sophisticated enough to sell on the Internet." *Id.* at 475.

In *State v. Heckel*, 24 P.3d 404 (Wash. 2001), *cert denied*, 534 U.S. 997 (2001), the Washington Supreme Court rejected a commerce clause challenge to that state's email spam legislation. There, an Oregon resident sent spam email to Washington residents in violation of a Washington anti-spam statute. The spammer challenged the law under the commerce clause. The Court followed the two-tiered approach and first considered whether the legislation was facially discriminatory. Finding that the subject

act applied equally to in-state and out-of-state spammers, the Court properly held there was no facial discrimination.

Turning to the *Pike* balancing test, the Court then considered the act's local benefits against any alleged burden on interstate commerce. Finding that spam caused injury to Washington citizens, including internet service providers and email users, the Court determined that the State had a legitimate interest to protect. The Court found that protection of such local interests outweighed any impact on interstate commerce. *See, also, Ferguson v. Friendfinders, Inc.*, 94 Cal. App. 4th 1255 (1st Dist. 2002) (upholding California's anti-spam act against a challenge under the dormant commerce clause). In similar challenges to Utah's anti-spam act, this Court has upheld such legislation against challenges under the commerce clause. *Riddle v. EDirect, Inc.*, No. 020412654 (Utah Third District Court Slip Op. May 7, 2003) (Utah's spam legislation not facially discriminatory and party challenging legislation offered no facts for Court to effectuate *Pike* balancing test) (a copy is attached as Exhibit "A").

Pitaki and the other cases relied on by WhenU are distinguishable, in part, because they are "passive website" cases. In a passive website case, the person challenging a state law is located in another state and does not actively distribute offending material or take other action directed toward the applicable state. Rather, the person merely operates a website in another state that is accessible by anyone on the Internet, including citizens of the state with the subject legislation. Accordingly, under the law challenged in *Pitaki*, a website owner in Georgia could be held liable simply

because his website was viewable by someone in New York. Similarly, in *American Civil Liberties Union v. Johnson*, 194 F.3d 1149 (10th Cir. 1999), the Court was faced with a law that applied to passive website operators in other states.

This is not the present situation. The Spyware Act clearly is designed to prohibit affirmative acts – i.e., the secret installation of spyware or the targeting of websites. Such conduct is accomplished by the installation of computer code on Utah computers or which target Utah websites. The affirmative acts of secretly downloading software onto Utah computers cannot be compared to merely operating a website which Utah residents may choose to view. The Spyware Act is a proper exercise of Utah’s legislative function.

D. WhenU is Not Likely to Succeed on the Merits of its First Amendment Claim.

WhenU’s First Amendment right to commercial speech is not infringed by the Spyware Act.⁸ The First Amendment of the Constitution of the United States “as applied to the States through the Fourteenth Amendment, protects commercial speech from unwarranted governmental regulation.”⁹ *Central Hudson Gas & Elec. Corp. v. Public Service Comm’n*, 447 U.S. 557, 561 (1980). The First Amendment, however, “accords a lesser protection to

⁸ It is undisputed that the only type of speech at issue in this case is commercial speech, which has been defined as “expression related solely to the economic interests of the speaker and its audience.” *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 445 U.S. 557, 562 (1980).

⁹ Although WhenU asserts that the Spyware Act violates the free speech rights guaranteed under both the United States and Utah Constitutions, WhenU failed to set forth any separate legal analysis regarding the Act’s violation of the Utah Constitution. Therefore, WhenU has failed to properly raise its freedom of speech argument under the Utah Constitution. *See State v. Davis*, 972 P.2d 388, 392 (Utah 1998) (affirming Court of Appeals ruling that plaintiff had failed to properly raise claim under Utah Constitution because plaintiff had not adequately set forth any separate legal analysis and had “not otherwise suggested a reason that warrants a distinct analytical treatment under the Utah Constitution”).

commercial speech than the other constitutionally guaranteed expression.” *Id.* at 562-563. “The protection available for particular commercial expression turns on the nature both of the expression and of the governmental interests served by its regulation.” *Id.* at 563.

The Supreme Court in *Central Hudson* set forth and applied a four-part analysis to determine the constitutionality of government restrictions on commercial speech. *Id.* at 562-566. The first step is to determine whether the expression is protected by the First Amendment, which means that “it at least must concern lawful activity and not be misleading.” *Id.* at 566. Second, it must be determined whether the governmental interest is substantial. *Id.* Third, if the first two inquiries are answered affirmatively, the court “must determine whether the regulation directly advances the governmental interest asserted, and [fourth] whether it is not more extensive than is necessary to serve that interest.” *Id.* “The last two steps of the *Central Hudson* analysis basically involve a consideration of the ‘fit’ between the legislature’s ends and the means chosen to accomplish those ends.” *Posadas De Puerto Rico Assocs. v. Tourism Company of Puerto Rico*, 478 U.S. 328, 341 (1986).

Applying the *Central Hudson* four-step analysis to the Spyware Act establishes that the Act is not an unconstitutional restraint of commercial speech. The first inquiry under the *Central Hudson* analysis is to determine whether the commercial speech is entitled to First Amendment protection. Commercial speech is only protected from government regulation by the First Amendment if it is neither misleading nor related to unlawful activity. *See Central Hudson*, 447 U.S. at 563 (“The government may ban forms of communication more likely to deceive the public than to inform it, or commercial speech related to illegal activity.” (citations omitted)).

Commercial speech can be misleading not just because of what it says, but also due to the manner or context in which it is presented. The very commercial speech that the Spyware Act seeks to restrict is misleading because it deceives or confuses the consumer, who is unaware that the spyware software has been installed on his or her computer, as to the affiliation, connection or association of the advertisement to the web site or web page that the consumer is viewing. The potential for the consumer to be misled by spyware targeted pop-ups is significant and has been substantiated through surveys conducted on that precise issue. Accordingly, because the commercial speech the Spyware Act seeks to restrict is misleading due to the manner and context in which it is presented, as well as its content, it does not merit First Amendment protection.

Not only is the use of targeted pop-ups that do not meet the identification provisions of the Act misleading, it also relates to unlawful activity since the use of such advertising likely constitutes at least the following unlawful activities: trademark infringement, unfair competition, trademark dilution, copyright infringement, misappropriation, interference with prospective economic advantage and unjust enrichment. For example, unfair competition under Section 43(a) of the Lanham Act, makes it unlawful for a person to, *inter alia*, use any word, term, name, symbol, or device that is likely to cause confusion or to deceive “as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.” 15 U.S.C. § 1125(a)(1)(A). Unfair competition involves any “deceptive marketing” or “appropriation of intangible trade values” that tends to mislead the public. Restatement (Third) of Unfair Competition § 1(a) (1995). Targeted pop-ups that do not “clearly identify” the source as

required by the Spyware Act confuses or is likely to confuse consumers concerning the “affiliation, connection, or association” of the contextually triggered advertisements to the website visited. That is the essence of unfair competition under the Lanham Act.

Even if the commercial speech that the Spyware Act targets is not misleading or related to unlawful activity and is subject to the First Amendment’s lesser protection afforded commercial speech, the Spyware Act is constitutional. The second step in the *Central Hudson* analysis inquires into whether the challenged law advances a substantial government interest. WhenU mistakenly identifies the governmental interest advanced by the Spyware Act as the protection of the privacy rights of computer users. The substantial government interests advanced by the Spyware Act are (1) to prevent the unauthorized installation of software on the computers of Utah residents and the accompanying unauthorized utilization and monitoring of their computer use; and (2) to protect businesses operating in Utah from deceptive trade practices and unfair trade practices. It can hardly be disputed that Utah has a substantial interest in protecting those individuals within its borders from the unauthorized interference with the use of their computers, as well as a substantial interest in protecting businesses that operate in Utah from deceptive trade practices and unfair competition. Courts have consistently recognized that States have legitimate and substantial interests in advertising and fair competition. *See, e.g., In re Utah State Bar Petition*, 647 P.2d 991, 995 (Utah 1982) (noting substantial state interest in avoiding false, deceptive, or misleading advertising for legal professionals); *Friedman v. Rogers*, 440 U.S. 1, 15 (1979) (“It is clear that the State’s interest in protecting the public from the deceptive and misleading use of optometrical trade names is substantial and well

demonstrated.”); *Tykla v. Gerber Products, Co.*, 182 F.R.D. 573, 578 (N.D. Ill. 1998) (noting that “the State of Illinois has a significant interest in preventing fraudulent and deceptive business practices within its borders”).

The fact that the Spyware Act does not specifically state the governmental interest advanced by the Act, does not in any manner limit the Court’s ability to find a governmental interest. The United States Supreme Court in *Posadas* affirmed a Puerto Rico statute based in part on Puerto Rico’s Superior Court’s determination of a governmental interest and a judicial narrowing of the statutory language to better fit the newly identified governmental intent. 478 U.S. at 334-335, 340-41. Specifically, the Superior Court determined that the legislature was worried about the welfare of its residents causing it to ban completely casino gambling advertising directed at Puerto Rico’s citizens. *Id.* Based on the implied governmental interest, the Superior Court narrowed the language of the statute to fit that interest. *Id.*

The third and fourth steps of the *Central Hudson* analysis, as stated above, “basically involve a consideration of the ‘fit’ between the legislature’s ends and the means chosen to accomplish those ends.” *Id.* at 341 (affirming lower court’s upholding of Puerto Rico’s ban of casino gambling advertising directed at Puerto Rico’s citizens). Specifically, the third step considers “whether the regulation directly advances the governmental interest asserted” *Central Hudson*, 447 U.S. at 566. As identified above, Utah has a substantial interest in preventing the unauthorized installation and utilization of software on the computers of Utah residents and to protect businesses operating in Utah from deceptive trade practices and unfair competition. The Spyware Act directly advances those interests by prohibiting the unauthorized

installation and utilization of software on a computer that causes the unauthorized displaying of advertisements in response to specific web sites or web pages visited, without obtaining the informed consent of the computer user. Utah Code Ann. § 13-39-101, *et. seq.* In short, the Spyware Act by requiring informed consent directly restricts the unauthorized installation and utilization of software and deceptive trade practices and unfair competition, which are substantial government interests.

The fourth step of the *Central Hudson* analysis, and the second half of the “fit” inquiry, is whether the regulation is no more extensive than necessary to serve the government’s interest. 447 U.S. at 566. Notably, this is not a “least restrictive means” inquiry, but, instead, “a ‘fit’ between the legislature’s ends and the means chosen to accomplish those ends – a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is ‘in proportion to the interest served;’ that employs not necessarily the least restrictive means but . . . a means narrowly tailored to achieve the desired objective.” *Board of Trustees of the State U. of New York v. Fox*, 492 U.S. 469, 480 (1989) (affirming Court of Appeal’s remand to District Court to make further factual findings in order to determine whether the government restriction was more extensive than necessary).

The Spyware Act is narrowly tailored to fulfill the purposes listed above and is not more restrictive than necessary. For example, the Act only applies to software downloaded without informed consent on a computer that monitors the computer’s usage; sends information about the computer’s usage to a remote computer or server or displays or causes to be displayed an

advertisement in response to the computer's usage through a triggering mechanism. Utah Code Ann. § 13-39-102(4).

WhenU makes no effort to suggest less restrictive means to achieving the governmental interests that are actually sought to be advanced by the Spyware Act. Instead, WhenU, once again, attempts to limit the governmental interest sought to be advanced to privacy of personal information and argues that the privacy could be achieved through a law restricting the information companies can collect about computer users. However, such a law would do nothing to prevent the primary evil the Act targets – namely, the unauthorized installation and utilization of software on the computers of Utah residents and the deceptive trade practices and unfair competition sought to be restricted by the Spyware Act.

WhenU's argument that the Act is over inclusive because it completely eliminates entire channels of communication is far from the truth. WhenU and other affected entities remain free to continue to utilize contextual advertising as an advertising medium, but must do so in compliance with the terms of the Act. In fact, the only restriction is placed on the use of targeted pop-ups that obscure the targeted websites. WhenU, and other "contextual" marketing companies, can easily use all other means to send their contextual messages to consumers, including pop-uppers,¹⁰ email, etc. Any burden associated with complying with the Act is outweighed by the legitimate government interests served by the Act.

WhenU also attempts to characterize the Act's restrictions on contextual advertising software as a content based restriction. The exact opposite is true. Although the content of the

¹⁰ A pop-upper is simply a browser window that appears under the targeted website. Therefore, although sent to a computer user at the same time the user views a selected website, it does not obscure the targeted website.

advertisement is relevant to the deceptive trade practices and unfair competition the Act seeks to prevent, it is the method or manner in which the advertisements are presented, and not their content, that is targeted by the Act. To that end, all unauthorized contextual triggering software is prohibited by the Act, regardless of the content of the advertisements that would be triggered by the software. Accordingly, the Act is content neutral.

This Court should hold that WhenU is not likely to succeed on the merits of its First Amendment claim and, therefore, deny its application for a preliminary injunction on the grounds of its First Amendment claim.

E. WhenU is Not Likely to Succeed on the Merits of its Uniform Operation of Laws Claim Under Article I, Section 24 of the Utah Constitution.

The Spyware Act does not violate Article I, Section 24 (“Uniform Operation of Laws”) of the Utah Constitution because it has uniform operation. The Uniform Operation of Laws provision states: “[a]ll laws of a general nature shall have uniform operation.” Utah Constitution, Article I, Section 24. “The essence of this constitutional provision is the settled concern of the law that the legislature be restrained from the fundamentally unfair practice of classifying persons in such a manner that those who are similarly situated with respect to the purpose of the law are treated differently by that law, to the detriment of some of those so classified.” *Gallivan v. Walker*, 2002 UT 89, ¶16, 54 P.3d 1069 (internal quotation marks omitted). “In conducting an analysis of a challenged statutory provision under article I, section 24, ‘the broad outlines of the analytical model used in determining compliance with the uniform operation of laws provision remain the same in all cases, [but] the level of scrutiny we give

legislative enactments varies.” *Id.* at ¶39 (alteration in original) (quoting *Blue Cross & Blue Shield of Utah v. State*, 779 P.2d 634, 637 (Utah 1989)). The courts utilize the following three part analysis in determining whether the legislative enactment is unconstitutional under the uniform operation of laws provision:

(1) whether the classification is reasonable, (2) whether the legislative objectives are legitimate, and (3) whether there is a reasonable relationship between the [classification and the legislative purpose].

Ryan v. Gold Cross Services, Inc., 903 P.2d 423, 426 (Utah 1995).

Where the legislative enactment “implicates a fundamental or critical right or creates classifications which are considered impermissible or suspect in the abstract, [the Courts] apply a heightened degree of scrutiny.” *Gallivan*, 2002 UT 89, ¶23 (internal quotation marks omitted). Although the analytical framework is the same when applying a heightened degree of scrutiny, the second step requires a showing that the classification “has more than a speculative tendency to further the legislative objective and, in fact, actually and substantially furthers a valid legislative purpose.” *Lee v. Gaufin*, 867 P.2d 572, 582-583 (Utah 1993). “In other words, in order for a discriminatory classification to be constitutional, it must be reasonably necessary to further, and in fact must actually and substantially further, a legitimate legislative purpose.” *Gallivan*, 2002 UT 89, ¶25.

WhenU incorrectly assumes that the Spyware Act implicates a fundamental or critical right, presumably commercial speech. However, as addressed in the previous section, the commercial speech the Spyware Act targets is misleading and related to unlawful activity and,

therefore, does not merit protection under the First Amendment. Accordingly, Spyware Act does not implicate fundamental or critical rights.

Even if the Spyware Act does implicate a fundamental or critical right, the Act's classifications are reasonably necessary to further and in fact do actually and substantially further, a legitimate purpose and, therefore, survive the heightened scrutiny.

WhenU asserts that the Spyware Act creates the following three classifications that violate the Uniform Operation of Law provision of the Utah Constitution: (1) the class of entities or individuals that can bring actions for violations of the Spyware Act, which excludes both a private right of action and government enforcement; (2) the class of advertising entities providing contextual advertising that are restricted by the Act, which excludes website owners; and (3) the inclusion of contextual advertising software that is not "Spyware," but is still subject to the restrictions of the Act. Each of these classifications, to the extent they are actual classifications made by the Spyware Act, are reasonably necessary and do in fact substantially further the legitimate legislative purpose of the Spyware Act and, therefore, do not violate the Uniform Operation of Laws provision of the Utah Constitution.

It bears repeating that the primary legislative purpose of the Spyware Act is (1) to prohibit the unauthorized installment of contextual advertising software on the computers of Utah residents, and (2) to protect Utah business entities from deceptive trade practices and unfair competition. The first classification and exclusion identified by WhenU concerning those entities that are authorized to bring actions to enforce the Act, is reasonably necessary and substantially furthers the legislative purpose of the Act. In order to ensure that the purposes of

the Act are achieved, the Act authorizes those entities to bring actions for violations of the Act that, in the view of the Utah legislature, have the greatest interest in seeking its enforcement, which are Internet website owners or registrants, trademark or copyright owners, and authorized advertiser on an Internet website. Utah Code Ann. § 13-39-301. Contrary to WhenU's assertion of no State involvement and in furtherance of the Act's legislative intent, the Act provides that the Division of Consumer Protection will undertake an information gathering and evaluation role in the enforcement of the Act by establishing procedures whereby a person may report violations of the Act. Utah Code Ann. § 13-39-401.

The second classification objected to by WhenU is the class of contextual advertisers targeted by the Act and the exclusion of contextual advertising displayed by website owners. It is not the purpose of the Act to limit website owners from choosing to sell advertising space on their own website.¹¹ Rather, the Act is clearly designed to prevent the unfair practice of others using targeting software to get a free ride in the intellectual property and websites of others, even those who do not allow advertising on their sites. In light of the actual purpose of the Act, the classification is necessary to actually and substantially further that legislative purpose.

WhenU's final classification objection is that the Act includes contextual advertising software that is not "Spyware." This argument is also based on WhenU's erroneous assumption of the purpose of the Spyware Act, as well as WhenU's own definition of spyware, both of which are clearly not in accordance with the Act. The Act specifically defines Spyware as

¹¹ In addition, in the case of pop-up advertisements generated by the website owner that the computer user has voluntarily chosen to view, the advertisement comes from that very website. In that case, the website owner controls the manner, number and type of advertising that is shown on its site. In the case of a WhenU targeted pop-up, the advertisement is not generated by the website selected by the user, but by WhenU.

software on a computer that monitors a computer's usage, which includes, but is not exclusively limited to, software that "sends information about the computer's usage to a remote computer or server." Utah Code Ann. § 13-39-102(4). The Act's definition also encompasses software that "causes to be displayed an advertisement in response to the computer's usage . . ." regardless of whether it collects the personal information of the computer user. *Id.* Given that the legislative purpose of the Act is to prevent the unauthorized installment and utilization of "Spyware" software on a user's computer and to protect entities conducting business in Utah from deceptive trade practices and unfair competition, the inclusion of software that does not collect personal information is reasonably necessary and does in fact substantially further the legitimate legislative purposes of the Act.

The Spyware Act, as almost all legislation necessarily does, creates a number of classifications to achieve its intended purpose. However, the classifications created by the Act are reasonably necessary and do in fact substantially further the legitimate legislative purpose of the Act and, therefore, do not violate the Uniform Operation of Laws provision of the Utah Constitution.

F. When U Is Not Likely To Succeed On The Merits Of Its Claim Of Preemption Under Federal Copyright Law.

Sections 13-39-201 and 13-39-301 of the Spyware Act are not preempted by federal copyright law. Section 301(a) of the Copyright Act states:

[A]ll legal or equitable rights that are equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103 .

. . . whether published or unpublished, are governed exclusively by this title. . . .
[N]o person is entitled to any such right or equivalent right in any such work
under the common law or statutes of any State.

17 U.S.C. § 301(a) (2004). Section 301(b) clarifies what is implied by § 301(a) in stating
“[n]othing in this title annuls or limits any rights or remedies under the common law or statutes
of any State with respect to . . . activities violating legal or equitable rights that are not equivalent
to any of the exclusive rights within the general scope of copyright as specified by section 106.”

17 U.S.C. § 301(b). A copyright owner’s exclusive rights specified by § 106 are to: “(1)
reproduce the copyrighted work, (2) prepare derivative works; (3) distribute copies, (4) perform
the work publicly, and (5) display the work publicly.” *Kindergartners Count, Inc. v. Demoulin*,
171 F. Supp. 2d 1183, 1190 (D. Kan. 2001).

Regarding preemption by federal copyright law, “[t]here is well-settled precedent to
determine whether a state-law claim is preempted by federal copyright law.” *Carson v. Dynegy*,
344 F.3d 446, 456 (5th Cir. 2003). Generally, in addressing copyright preemption the courts
apply the following two-part analysis: “[f]irst, the claim is examined to determine whether it falls
within the subject matter of copyright as defined by 17 U.S.C. § 102. And second, the cause of
action is examined to determine if it protects rights that are equivalent to any of the exclusive
rights of the federal copyright, as provided in 17 U.S.C. § 106.” *Id.* (internal quotations and
citations omitted).¹² A statute is equivalent to any of the exclusive rights within the general

¹² 17 U.S.C. § 102 states in relevant part:

- (a) Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression. . . . Works of authorship include the following categories:
 - (1) literary works;

scope of copyright as specified by section 106 “if the act or acts of [the defendant] about which [the plaintiff] complains would violate both [state law] and copyright law. . . . If, however, one or more qualitatively different elements are required to constitute the state-created cause of action being asserted, then the right granted under state law does not lie ‘within the general scope of copyright,’ and preemption does not occur.” *Dorsey v. Money Mack Music, Inc.*, 304 F. Supp. 2d 858, 863 (E.D. La. 2003) (alterations in original; emphasis added) (quoting *Computer Management Assistance Co. v. Robert F. Decastro, Inc.*, 220 F.3d 396, 404 (5th Cir. 2000)). This equivalency inquiry is generally referred to as the “extra element” test and is widely accepted and utilized to uphold State statutes. *See, e.g., Kindergartners*, 171 F. Supp. 2d at 1190-1192 (holding that State unfair competition claim required extra element(s) and, therefore, was not preempted by federal copyright law); *Dun & Bradstreet Software Services, Inc. v. Grace Consulting, Inc.*, 307 F.3d 197, 216-219 (3rd Cir. 2002) (reversing lower court preemption holding because State misappropriation of trade secrets claim required extra element(s)); *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*, 9 F.3d 823, 846-848 (10th Cir. 1993) (same).

Applying this two-part test to §§ 13-39-201 and 13-39-301 of the Spyware Act amply shows that federal copyright law does not preempt them. The portion of § 13-39-201 targeted by WhenU’s preemption argument prohibits the “use of context based triggering mechanism to

-
- (2) musical works, including any accompanying words;
 - (3) dramatic works, including any accompanying words;
 - (4) pantomimes and choreographic works;
 - (5) pictorial, graphic, and sculptural works;
 - (6) motion pictures and other audiovisual works;
 - (7) sound recordings; and
 - (8) architectural works.

display an advertisement that partially or wholly covers or obscures paid advertising or other content on an Internet website in any way that interferes with a user's ability to view the Internet website." Utah Code Ann. § 13-39-201. Section 13-39-301 provides that "an action for a violation of this chapter may be brought . . . by . . . a trademark or copyright owner. . . ." Utah Code Ann. § 13-39-301. Assuming, for purposes of this argument only, that these sections fall within the subject matter of copyright as defined by 17 U.S.C. § 102 and, thus, satisfy the first part of the copyright preemption analysis, the next question is whether the sections are equivalent to any of the exclusive rights within the general scope of federal copyright law. The answer to that question is an absolute and unequivocal no.

The prototypical copyright action is for copyright infringement, which requires the proof of two elements, (1) ownership of the copyrighted material, and (2) copying by the defendant. *See Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 361 (1991). Although the Spyware Act seeks to protect the ownership interests of the website owners and advertisers from advertisements that are contextually triggered by software that has been installed on the computers of Utah residents, the Act as a whole, and the two challenged sections in particular, are not dependent on whether the content of the website is copyrighted or whether the website owners or advertisers own the copyrighted material. Nor does the Act require any copying, distribution, display or performance of copyrighted material. Accordingly, the facts that would support a claim under §§ 13-39-201 and 13-39-301 do not necessarily support a claim under the copyright laws and, therefore, are qualitatively different and cannot be held to be equivalent. *See Carson*, 344 F.3d at 456 ("If one or more qualitatively different elements are required to

constitute the state-created cause of action being asserted, then the right granted under state law does not lie within the general scope of copyright, and preemption does not occur.” (internal quotations and citation omitted)). WhenU has itself taken the position that copyright law does not apply to context based triggering software that displays, or causes to be displayed, advertisements that partially or wholly cover or obscures paid advertising or other content on an Internet website. *See, e.g., U-Haul International, Inc. v. WhenU.com, Inc.*, 279 F. Supp. 2d 723, 729-731 (E.D. Va. 2003). WhenU’s suggestion to this Court that the State’s regulation of such actions are now preempted by copyright law is disingenuous.

Even if this Court were to incorrectly hold that it is likely that the Spyware Act is equivalent to any of the exclusive rights within the general scope of federal copyright law, there are sufficient “extra elements” to preclude preemption. For example, the Spyware Act specifically targets the unauthorized installation and utilization of software that “use[s] a context based triggering mechanism to display an advertisement that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user’s ability to view the Internet website.” Utah Code Ann. § 13-39-201(c). Accordingly, a necessary element of the violation of § 13-39-201(c) is the use of a context based triggering mechanism, which is not a necessary element of a copyright infringement claim. Also, the Spyware Act, in seeking to restrict unauthorized contextual based triggering of advertising that partially or wholly covers or obscures paid advertising or interferes with a user’s ability to view the website, is concerned with protecting paid advertisers from having the view of their advertising, regardless of whether it is copyrighted, obscured. Protection for the viewing of

copyrighted material is not a protected copyright use as specified by § 106 of the Copyright Act and, therefore, is a “extra element.” In reality, the Act is more akin to a regulation restricting the placing of a billboard five feet in front of an existing billboard, which would severely limit the utility and value of obstructed billboard, but would not affect its copyrighted content, if any.

Finally, implicit in the Spyware Act is that when a computer user is unaware that context based triggering software has been installed on his or her computer, the advertisements that are triggered will cause confusion, mistake or deception as to affiliation, connection or association of the triggered advertisement to the website being viewed. Confusion, mistake or deception are elements outside the scope of copyright law which preclude preemption. *See, e.g., Kindergartners*, 171 F. Supp. 2d at 1192 (holding that the unfair competition claim brought by plaintiff was not preempted by federal copyright law because the claim asserted that use of plaintiff’s copyrighted program caused confusion, mistake and deception, which are not elements of copyright infringement, but instead, constituted “extra elements”).

The inclusion of copyright holders as individuals or entities entitled to bring an action for violation of the Spyware Act is not an attempt to create an alternate avenue for copyright enforcement, but is simply a recognition that they, along with Internet website owners or registrants, trademark owners, and authorized advertisers on an Internet website are likely to have the greatest interest in enforcing the legitimate State interests of the Spyware Act. It is beyond dispute that a statutory provision may designate the classes of individuals or entities that may bring claims for its enforcement when it serves the legitimate government interests of statute. Notably, a copyright owner would still be required to demonstrate a valid claim under

the Act, which as shown above requires more than ownership of copyrighted material and copying by the defendant. *See* Utah Code Ann. § 13-39-201.

Not only is the Spyware Act not preempted under the copyright specific preemption analysis, the Act is also not preempted under application of the well-established general test to determine federal preemption of state laws, which has been adopted by Utah. *See Utah v. Frampton*, 737 P.2d 183, 190-91 (Utah 1987) (holding that the Lanham Act does not preempt Utah's ability to recognize and protect trademark rights). This general preemption test applies the following three-factor test to determine if a state law has been federally preempted:

1. a state regulation is preempted where an unambiguous congressional mandate exists to that effect;
2. preemption exists where the state regulation cannot be enforced without impairing federal superintendence of the field; and
3. preemption of the state regulation exists where it stands as an obstacle to the accomplishment and execution of the full purposes of Congress.

Id. at 190. Utah recognizes that there is a general presumption against finding preemption. *Id.* (citing *Florida Lime & Advocado Growers, Inc. v. Paul*, 373 U.S. 132 (1963)).

Applying the *Frampton* general preemption test to the Spyware Act mandates the same result as the federal copyright preemption analysis. Regarding the first element, there is no unambiguous congressional mandate dictating federal copyright preemption of the Spyware Act. In particular, § 301(a) of the Copyright Act, which addresses federal copyright preemption, does not unambiguously mandate preemption of the Spyware Act and, in fact, mandates a finding of no preemption because the Spyware Act is not equivalent to any of the exclusive rights of federal copyright law, as addressed above.

The second and third elements of the general preemption test are likewise not met because the Spyware Act does not impair the federal superintendence of the field of copyright law and does not stand as an obstacle to the accomplishment and execution of the full purposes of Congress. Federal copyright law provides protection to the owner of original works of authorship fixed in any tangible medium from reproduction, derivative use, distribution, public performance and display. *See* 17 U.S.C. §§ 102 & 106. The Spyware Act operates irrespective of whether the content of a website or advertisement is an original work of authorship. If a website or advertisement infringes on a copyright, the copyright holder would be free to bring an action for infringement regardless of any violation of the Spyware Act. Nor does the Spyware Act permit the reproduction, derivative use, distribution, public performance or display of copyrighted works. Accordingly, the second and third elements are not met. *See Frampton*, 737 P.2d at 190 (holding that second and third elements of general preemption test were not met where the trademark owner remained free to seek redress under the Lanham Act and the state law did not permit actions in violation of the Lanham Act).

II. THE SPYWARE ACT WILL NEITHER CAUSE IRREPARABLE HARM TO WHENU NOR WOULD AN INJUNCTION BE IN THE PUBLIC INTEREST.

WhenU overstates the burdens the Spyware Act would impose on it. According to WhenU, the Spyware Act would force WhenU to change its business model on a nation-wide basis.¹³ This is simply not true. There are a number of ways WhenU can determine the location of the computer upon which its spyware will be installed. The Zip

¹³ WhenU also complains that the Utah act would subject WhenU to the potential of different regulatory schemes among the states. That is a natural by-product of doing business in different states.

Code information already gathered by WeatherCast in its install procedures is simply one of several options. It would be a simple matter to simply make sure that users in a Utah zip code were provided informed consent prior to downloading the WhenU software.¹⁴ In fact, WhenU currently determines the location of computers accessing its servers.

Similarly, WhenU states that the Spyware Act would have the effect of eliminating contextual advertising over the Internet. The Act simply prohibits pop-up advertisements that obscure other targeted websites. Contextual advertisers who do not unfairly target another's website through the use of obscuring pop-up advertisements are free to use a host of other advertising means, such as pop-unders, email, etc. Unless WhenU's business model is singularly dependant on the use of deceptive pop-up advertisements designed to lure users away from their selected websites, the effect on WhenU by the Spyware Act is minimal.

If WhenU is truly not causing its software to be downloaded without informed consent and the other protections of the Act, it will suffer no irreparable injury. In addition, the secret installation of spyware or the use of pop-up advertisements designed as a parasite on the intellectual property and websites of others is not sanctioned under existing law. WhenU itself acknowledges the existence of other laws affecting such conduct. (WhenU Memorandum, at 15, 23). A law which prohibits improper conduct clearly cannot cause irreparable harm.

¹⁴ Providing informed consent seems a laudable business goal in any event.

CONCLUSION

The Spyware Act addresses valid local concerns caused by the improper installation of spyware on Utah computers and the unfair targeting of websites owned by Utah businesses. WhenU cannot satisfy its very high burden of establishing, without a reasonable doubt, that the Act is unconstitutional. The requested preliminary injunction should not issue.

Dated this 18th day of May 2004.

Miller Magleby & Guymon, P.C.



Blake D. Miller
Paxton R. Guymon
Joel T. Zenger
Special Assistant Attorneys General
Attorneys for Defendants

CERTIFICATE OF SERVICE

I hereby certify that I am employed by the law firm of MILLER MAGLEBY & GUYMON, P.C., 170 South Main Street, Suite 350, Salt Lake City, Utah 84101, and that pursuant to Rule 5(b), Utah Rules of Civil Procedure, a true and correct copy of the foregoing **MEMORANDUM IN OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION** was delivered to the following this 18th day of May by:

- Hand Delivery to Alan Sullivan ONLY
- Facsimile
- Depositing the same in the U.S. Mail, postage prepaid
- Federal Express
- Certified Mail, Receipt No. _____, return receipt requested

Brent V. Manning
Douglas R. Larson
MANNING CURTIS, BRADSHAW
& BEDNAR, LLC
Third Floor Newhouse Building
10 Exchange Place
Salt Lake City, UT 84111

Alan L. Sullivan
James D. Gardner
SNELL & WILMER
15 West South Temple, Suite 1200
Gateway Tower West
Salt Lake City, UT 84101-1004

Celia Goldwag Barenholz
Michael D. Paley
KRONISH LIEB WEINER & HELLMAN, LLP
1114 Avenue of the Americas
New York, NY 10036

A handwritten signature in black ink, appearing to be "AS", written over a horizontal line.

Exhibit “A”

IN THE THIRD JUDICIAL DISTRICT COURT
IN AND FOR SALT LAKE COUNTY, STATE OF UTAH
SANDY DEPARTMENT

JESSE RIDDLE,

Plaintiff,

vs.

EDIRECT, INC. dba DIRECT DEBT
CONSOLIDATION.COM and JOHN
DOES one through ten whose true names
are unknown,

Defendants

FILED
THIRD DISTRICT COURT
SANDY DEPT.
5-7-03

DEAN BECKER,

Plaintiff,

vs.

LOWERMYBILLS.COM and JOHN
DOES one through ten whose true
names are unknown,

Defendants

MEMORANDUM DECISION AND
ORDER DENYING DEFENDANTS'
MOTIONS TO DISMISS FOR FAILURE
TO STATE A CLAIM FOR RELIEF

Case Nos 020412654
020405511
020413665
020413677
020413643
020413676
030400429

RICH THOMSON,

Plaintiff,

vs.

EDIRECT, INC. dba DIRECT DEBT
CONSOLIDATION.COM and JOHN
DOES one through ten whose true
names are unknown,

Defendants

BRETT DAVIS, individually and on
behalf of others similarly situated,

Plaintiffs,

vs.

Judge Denise Posse Lindberg

APOLLO GROUP, INC., and JOHN
DOES one through ten whose true names
are unknown,

Defendants

CHIP ORMOND, on behalf of himself and
all others similarly situated,
Plaintiffs,

vs

APOLLO GROUP, INC. and JOHN
DOES one through ten whose true names
are unknown,
Defendants

BRITTANY HUGHES, individually and on
behalf of others similarly situated,

vs

APOLLO GROUP, INC., and JOHN
DOES one through ten whose true names
are unknown,
Defendants

JASON MEISTER, an individual,
Plaintiff,

vs

¶7 Moreover, in considering these Combined Motions the Court must keep in mind its duty to interpret statutes so as to uphold their constitutionality whenever possible. See e.g. *Mountain States Te. & Tel. Co. v. Payne*, 782 P.2d 464, 467 (Utah 1989).

ANALYSIS

¶8 Plaintiffs' Complaints make the following substantive allegations:

- (1) That Defendants conduct portions of their businesses "by sending unsolicited e-mails into the State of Utah";
- (2) That Defendants "sent, or caused to be sent," to Plaintiffs one or more unsolicited emails as defined in the Act;
- (3) That the emails were "commercial email" as defined in the Act;
- (4) That the emails were "unsolicited" as defined in the Act; and
- (5) That the emails sent to the various Plaintiffs "failed to comply with one or all of the requirements" of the Act.

E.g. Thomson Complaint, ¶¶ 2, 6-9.

¶9 Defendants do not (and, indeed, given the procedural posture of the case, cannot) dispute Plaintiffs' allegations, which the Court accepts as true for purposes of resolving these Combined Motions.

¶10 These allegations, bare-bones though they may be, clearly state a claim under the Act. Arguably, however, a question remains whether Plaintiffs, relying on an allegedly unconstitutional Act, can state a claim for relief. Utah R. Civ. P. 12(b)(6).

Facial challenge under "dormant" Commerce Clause.

¶11 Defendants allege that the Act violates the negative or dormant Commerce Clause of Article I of the United States Constitution. See *Cooley v. Board of Wardens*, 12 How. 299, 53 U.S. 299 (1851). By its terms, the Constitution grants Congress the power "to regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." U.S. Const. art. I, §8, cl. 3. By negative implication, the Supreme Court has interpreted the Commerce Clause not only as an authorization for congressional action, but also, even in the absence of a conflicting federal statute, as a restriction on permissible state regulation." *Hughes v. Oklahoma*, 441 U.S. 322, 326 (1979).

¶12 This "negative" or "dormant" aspect of the Commerce Clause prohibits States from "advancing their own commercial interests by curtailing the movement of articles of commerce

either into or out of the state." *Fort Gratiot Sanitary Landfill, Inc., v. Michigan Dep't of Natural Res.*, 504 U.S. 353, 359 (1992) (quoting *H.P. Hood & Sons, Inc., v. Du Mond*, 226 U.S. 525, 535 (1949)). "The central rationale for the rule against discrimination is to prohibit state laws whose object is local economic protectionism, laws that would excite those jealousies and retaliatory measures the Constitution was designed to prevent." *C & A Carbone, Inc., v. Clarkstown*, 511 U.S. 383, 390 (1994).

¶13 Statutes challenged under the dormant Commerce Clause are first analyzed as to whether or not they discriminate against interstate commerce. If a challenged statute imposes "differential treatment of in-state and out-of-state economic interests that benefits the former and burdens the latter," *Oregon Waste Systems, Inc., v. Department of Environmental Quality of Ore.*, 511 U.S. 93, 99 (1994), the courts apply "a virtually per se rule of invalidity." *Environmental Technology Council v. Sierra Club*, 98 F.3d 774, 784 (4th Cir. 1996). By contrast, a statute that regulates "evenhandedly" and only indirectly affects interstate commerce is treated more deferentially. Such a statute is assumed to be "valid unless the burdens on commerce are 'clearly excessive in relation to the putative local benefits.'" *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970).

¶14 On its face, nothing in the challenged Act clearly discriminates against interstate commerce. The Act's requirements apply evenhandedly to anyone who "sends, or causes to be sent, an unsolicited commercial email . . . through the intermediary of an email service provider located in the state or to an email address held by a resident of the state." Utah Code § 13-36-103(1). Stated another way, the requirements imposed by the Act apply equally to senders of UCEs, whether or not those email messages initiate within, or outside of Utah. Since the statutory language is not facially discriminatory, the more deferential analysis (which presumes validity of the statute), applies. Only if the burdens of commerce are "clearly excessive in relation to the putative local benefits," will the statute be found unconstitutional. "[T]he extent of the burden that will be tolerated will, of course, depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities." *Pike v. Bruce Church*, 397 U.S. at 142.

¶15 At this stage of the proceedings, the Court's record includes no facts on which the Court can rely to balance the benefits and burdens associated with the Act.² Without such facts, the *Pike* balancing test simply cannot be done.³ As a result, the Court cannot determine conclusively that there is no "state of facts [Plaintiffs] could prove to support their claim[s]." *Educators Mut. Ins. Ass'n v. Allied Property & Cas. Ins. Co.*, 890 P.2d at 1030. Accordingly, Defendants' R. 12(b)(6) argument of facial unconstitutionality must fail.

²Following oral argument each side submitted various letters from counsel, with attached documents. None of those submissions included factual affidavits, and have not been considered by the Court in ruling on these Combined Motions.

³Defendants have failed to indicate to the Court how a "facial challenge" (which does not depend on specific facts) can be reconciled with the *Pike* balancing test, which requires facts on the record.

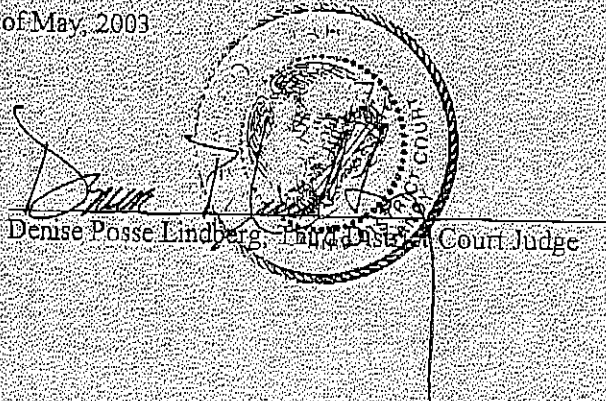
"As applied" challenge

¶16 The thrust of the argument raised by Defendants in these Combined Motions is that the Act's extraterritorial effects render the Act unconstitutional "as applied." Again, absent specific facts showing the Act's alleged extraterritorial effects, the Court is unable to assess the validity of those claims, or to determine conclusively that application of the Act to these Defendants would violate the dormant Commerce Clause. Accordingly, Defendants' Combined Motions to dismiss also fail under an "as applied" challenge.

ORDER

¶17 For the foregoing reasons, all of the present Defendants' Rule 12(b)(6) Motions to Dismiss (for failure to state a claim upon which relief may be granted) are DENIED.

So Ordered by the Court this 7th day of May, 2003.



Denise Posse Lindberg, District Court Judge