Washington Journal of Law, Technology & Arts

Volume 2 | Issue 4 Article 3

4-14-2006

The SPY Act: Ditching Damages as an Element of Liability for On-Line Conduct Between Private Parties?

Andrew T. Braff

Constitutional & Regulatory
Cite as: Andrew T. Braff, *The SPY ACT: Ditching Damages as an Element of Liability for On-Line Conduct Between Private Parties?*, 2 Shidler J. L. Com. & Tech. 17 (Apr. 14, 2006), *at* <http://www.lctjournal.washington.edu/Vol2/a017Braff.html>

THE SPY ACT: DITCHING DAMAGES AS AN ELEMENT OF LIABILITY FOR ON-LINE CONDUCT BETWEEN PRIVATE PARTIES?

Andrew T. Braff[1]

Abstract

The question of how to stymie the proliferation of *spyware* on computers has been a recurring topic of debate in Congress and in the technology industry. With the passage of the SPY ACT (H.R. 29) a high probability, this article highlights its prohibitions, with particular emphasis on how they change current legal regimes. Most federal computer statutes—insofar as they address actions victimizing private citizens—require *damage* to the computer. In addition, one of the elements of common law trespass to chattel is damage. Whether intended or not, the SPY ACT subtly introduces a strict liability component into federal computer and Internet law.

Table of Contents

INTRODUCTION

<1> Throughout 2004, a debate raged between Federal Trade Commission (FTC) commissioners[2] and Congress as to whether legislation was required to stymie the disturbing prevalence of *spyware* on computers.[3] To prove existing law adequate, the FTC commenced the first spyware action against Sanford Wallace and his affiliated corporations.[4] Those in the computer industry also expressed concern regarding the legislative approach, fearing spyware would be defined as a type of software and prohibited, and that certain beneficial technologies would thus be eliminated. Heeding these warnings, Congress discarded the definitional approach, choosing instead to prohibit questionable conduct[5] similar to that involved in *FTC v. Seismic Entertainment Productions, Inc.*[6] The House overwhelmingly passed the SPY ACT (H.R. 2929)[7] in October 2004, but the Senate failed to vote before the 108th Congress ended. As the 109th Congress commenced, Representative Mary Bono immediately reintroduced a slightly modified version bearing the same name.[8]

<2> New legislation yields two questions for practitioners: (1) are new offenses created that may impact a client's business model; and (2) are new causes of action created to redress harm to an individual's property? The short answer to the latter is *no*,[9] but the answer to the former is more complicated. Although H.R. 29 does not create a cause of action for private redress, it outlines specific conduct that expands liability in a subtle way; namely, the Act *does not* require that the conduct damage or harm property or the person in order to constitute a violation.

<3> If H.R. 29 is considered a "privacy" bill, then this lack of damage or harm element is nothing new. Other privacy statutes enforced exclusively by the government, such as HIPAA, COPPA, and Gramm-Leach-Bliley, do not require damage or harm to persons or property to constitute a violation. But discussions regarding the need for H.R. 29 frequently reference current laws on computer crime or hacking, rather than existing privacy law. As a result, the legal framework for approaching spyware naturally focuses on theories of conversion, trespass, fraud, theft, and federal statutes codifying these common law theories. Viewed in this context, H.R. 29 is a departure from current laws governing general computer crime and conduct on the Internet where measurable harm or damage is almost always an element of the offense. Those disseminating software having the characteristics of spyware must consider the implications of the privacy law approach taken by H.R. 29 and account for this subtle expansion of liability.

<4> This article analyzes the SPY ACT, particularly Sections 2 and 3, to determine its impact on common law and statutory regimes relating to computer intrusion and deceptive practices in

preparation for what, by most accounts, is the inevitable passage of federal legislation.[10]

CURRENT INTERNET LAW AND THE NECESSITY OF DAMAGE

<5> In the U.S., laws governing action between private parties on the Internet—whether common law trespass to chattel, or statutes such as the Federal Trade Commission Act (FTCA)[11] and the Computer Fraud and Abuse Act (CFAA)[12] —generally require *damage* in order to be cognizable either civilly or criminally.

Common Law

<6> At common law, a dispossession of or interference with personal property is governed primarily by the theories of conversion and trespass to chattel. Where the former involves complete dispossession of property, the latter governs partial disposition or interference "not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered."[13] Under a trespass to chattels theory, liability arises if there is dispossession —regardless of whether there is harm or damage to the chattel— or if "the chattel is impaired as to its condition, quality, or value, or the possessor is deprived of the use of the chattel for a substantial time."[14] Therefore, other than complete dispossession, no legal protection is given for 'harmless intermeddlings' unless they affect the possessor's "materially valuable interest in the physical condition, quality, or value" of the chattel resulting in some harm exceeding the nominal or dignitary.[15] Damage, therefore, is an element of liability.

<7> In the context of electronic communications, the California Supreme Court, in *Intel Corp. v. Hamidi*, found that Intel could not maintain a trespass to chattels action against a former employee for sending email messages to thousands of current employees via company email accounts. This tort "does not encompass … an electronic communication that neither damages the recipient computer system nor impairs its functioning."[16] Even though defendant Hamidi's messages "temporarily used some portion of the Intel computers' processors or storage … [Intel] does not demonstrate some measurable loss from the use of its computer system."[17] More importantly, the loss of productivity, or time spent fending off interferences with a computer's 'cycle time' that individually fail to impair the functionality of the computer cannot be "bootstrapped into injury to [a] possessory interest in [a] computer."[18] In sum, individual activities resulting in infinitesimal damage cannot form the basis

for liability.

Federal Trade Commission Act

<8> Spyware and adware often contain elements of fraud and deception. The FTCA declares unlawful "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[19] Although extremely broad, an act or practice is only "unfair" if it is "likely to cause *substantial injury* to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[20] Adware that collects information or monitors a user's web surfing habits in order to deliver targeted advertisements likely provides 'clickwrap' containing a privacy policy, end-user license agreement (EULA), and/or a Terms of Use agreement. The FTC has taken enforcement action against companies that have posted privacy policies and failed to comply with them.[21] Nevertheless, the first hurdle to FTC enforcement is a demonstration of substantial injury,[22] which is often easily debatable as seen in *FTC v. ReverseAuction.com, Inc*.[23]

Computer Fraud and Abuse Act

<9> The CFAA "facilitates addressing in a single statute the problem of computer crime."[24] It provides criminal sanctions for offenses against government and private computers, as well as an avenue for civil recourse for harm caused to private computers in certain situations.[25] The CFAA has evolved significantly since its original manifestation as the Counterfeit Access Device and Computer Fraud and Abuse Act, which protected classified information, financial records and credit information on government and financial institution computers (*federal interest* computers) from "unauthorized access" in addition to computer crime involving interstate commerce.[26] The statute did not reach harms to federal interest computers caused by other methods, including harm resulting from access by an "authorized" individual.[27] Civil penalties were added in 1994, allowing any person suffering damage to their computers to maintain a civil action.[28] In addition, the 1994 amendment "broadened the proscribed range of conduct to transmissions," thereby "shifting the focus towards the defendant's harmful intent and resulting harm, rather than the technical concept of computer access and authorization."[29] The term *protected computer*, which defines the subject of the CFAA's protection, has since been substituted in place of the federal interest computer.[30] This is one example of

Congress's further broadening of the CFAA's application.

<10> This article concerns actions between private parties on the Internet; therefore, it discusses only the sections of the CFAA pertaining to private computers. For a private computer to be a *protected computer* under CFAA, it must be used "in interstate or foreign commerce or communication."[31] A computer located outside the U.S. can also be protected by the CFAA if it is "used in a manner that affects interstate or foreign commerce or communications of the United States."[32] The advent of the Internet has rendered almost all computer use interstate in nature. All private computers infected with spyware are likely protected computers, since the process of contracting and the operation of spyware necessarily involve the Internet and interstate commerce.

<11> First, § 1030(a)(2)(c) of Title 18 punishes a person or entity that "intentionally accesses a computer without authorization or exceeds authorized access, and thereby *obtains* … information from any protected computer if the conduct involved an interstate or foreign communication."[33] Section 1030(b) prohibits *attempts* to commit such an action, which does not require damages for the government to bring an action. Rather, *authorization*—or a lack thereof—substitutes for damage to the owner's interest as a critical element for violating this section of the CFAA. However, this section does not necessarily enhance its utility in the context of spyware and adware. Current interpretations of authorization grant providers of this software a key defense because most monitoring software is downloaded via bundling and with the user's *consent*.[34] As discussed below, H.R. 29 may redefine what constitutes authorization, even though violations of H.R. 29 are to be enforced as unfair or deceptive trade practices under Section 5 of the FTCA.[35]

<12> Second, § 1030(a)(4) subjects to punishment any person who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value."[36] The "thing obtained" for value "may not merely be the unauthorized use" of the computer.[37] However, if the conduct consisted only of the use of the computer, the value of such use must exceed $5,000 in any 1-year period for the government to bring an action.[38]

<13> Finally, § 1030(a)(5) prohibits conduct that "intentionally causes damage" by knowingly accessing or transmitting information or code to a protected computer. [39] Here, damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information."[40] Unlike § 1030(a)(2),

information does not have to be obtained. A civil action for a violation of the CFAA may be brought only if the conduct falls under § 1030(a)(5) and involves $5,000 in "loss"[41] to one or more persons during a 1-year period; physical injury; threat to public health or safety; or impairment of a medical examination, diagnosis, treatment, or care of one or more individuals.[42]

<14> The common and statutory laws addressed above are logical avenues to redress conduct related to spyware. Such conduct often seems to constitute unauthorized computer intrusion or an intrusion that exceeds the user's authorization (i.e., a mixture of theft and trespass law modified by the CFAA to fit the virtual world), or potentially unfair or deceptive trade practices. Such conduct often yields a result that, in the aggregate, impairs the chattel. However, these avenues have proven inadequate due in part to their damage requirements. H.R. 29 subtly moves away from insulating actions that fail to cause damage or harm and instead moves toward prohibiting conduct based on a lack of consent—or getting consent in an improper way.

THE SPY ACT: DITCHING DAMAGE AS AN ELEMENT OF LIABILITY FOR PRIVATE PARTY CONDUCT

<15> The trend away from requiring damage as an element for unlawful conduct between private parties appears to have started subtly with the CAN-SPAM Act, which does not require damage as an element for its violation.[43] Punishment is predominantly based upon whether the violator has committed prior offenses, whether an offense under the Act was committed in furtherance of a felony, and the volume of Spam[44] sent by the violator. One penal provision does, however, provide for punishment by fine and/or imprisonment where the offense "caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period."[45] H.R. 29 continues this trend by rendering certain conduct unlawful despite a lack of cognizable damage.

Prohibitions

<16> Generally, the SPY ACT proscribes certain deceptive or surreptitious conduct associated with the placement and utilization of programs on a personal computer that monitor usage, collect information, and modify settings. Although there are nine categories of conduct prohibited in Section 2, a violation of the Act can fall under no less than twenty specific provisions in Sections 2 and 3. These are outlined in detail in Appendix A, and are enumerated and summarized here for purposes of easy reference. Sections 2 and 3 prohibit the following conduct by any person *not the owner or authorized user* of a protected computer (except Nos. 19 and 20, which also apply to the

owner/authorized user):

1. Taking control of the computer to Spam others;
2. Taking control of the computer by diverting the browser away from a website the user intended to view;
3. Taking control of the computer via use of a dialer [46] or Internet connection or service;
4. Using the computer as part of a group of computers ("bot farm") to perform an activity;
5. Delivering ads using browser windows that will not close;
6. Modifying the browser's default homepage;
7. Modifying settings used to access or search the Internet;
8. Modifying a browser's bookmarks;
9. Modifying security or other settings that protect information on the computer;
10. Collecting personally identifiable information via keystroke logging function;
11. Inducing installation by giving an option to decline software installation, but installing software even if it is declined;
12. Preventing uninstallation or deactivation via use of a Trojan[47] that automatically reinstalls;
13. Procuring installation or information by misrepresenting its necessity to access content;
14. Misrepresenting identity to procure installation or execution of a program;
15. Misrepresenting identity to procure information (personal, password, account);
16. Procuring information without the authority of the intended recipient of the information;
17. Interfering with security, anti-spyware, or anti-virus technology on the computer;
18. Installing a program with the intent of causing another person to violate the act;
19. Transmitting an "information collection program"; and

20. Executing an "information collection program."

<17> Some of these prohibitions can be circumvented by procuring authorization of either the owner of the computer (Nos. 2 and 18) or the intended recipient of information (No. 16). This latter provision may be used in situations similar to those in *In re DoubleClick Inc. Privacy Litigation*.[48] In this case, even though the placement of cookies[49] on the plaintiff class's computers constituted intentional access of a stored electronic communication without authorization in violation of the Electronic Communications Privacy Act, an exception is provided for conduct authorized by a user of the electronic communications service:[50] the affiliate web site who hired DoubleClick to deliver ads and cookies to its visitors.[51] The Wiretap Act provides a similar exception, allowing for intentional intercepts of electronic communications when one of the parties consents.[52]

Provisions Allowing for Information Collection Programs, Exemptions & Preemption

<18> More importantly, transmitting (No. 19) or executing (No. 20) information collection programs can still occur, provided a computer owner or authorized user is given the chance to "opt-in" after receiving proper notice and consent. An information collection program is defined as software that either:

1. "collects personally identifiable information and sends such information to a person other than the owner or authorized user of the computer," OR uses the information to deliver advertising; OR
2. "collects information regarding the Web pages accessed" in order to deliver advertising.[53]

The procedure for providing proper notice is outlined specifically and needs only be given once unless the information collected is "materially different" or "outside the scope" of previous authorization.[54] Aside from notice, the only other requirement is that the information collection program contains certain "required functions." These include an easily identifiable "disabling function" allowing a user to uninstall or disable the program "without undue effort or knowledge," and an "identity function," which provides a logogram or trademark of the information collection program when delivering advertisements while the owner or authorized user is visiting a website other than that owned by the program provider.[55]

<19> The SPY ACT contains several other standard exemptions for

law enforcement; carriers; operators; and providers of services to monitor security, diagnostics, repair, or fraudulent activity. The manufacturers and retailers of computer equipment are insulated from liability for the third-party branded software that comes installed on the computer. There is also a "Good Samaritan" provision for those providers of computer software violating sections 2 and 3 in order to remove the programs upon consent of the computer owner.[56] Finally, there is a somewhat murky preemption regime.[57]

Damage Requirements in the SPY ACT—Or Lack Thereof

<20> The SPY ACT borrows its definition of *damage* from the CFAA: "any impairment to the integrity or availability of data, a program, a system, or information."[58] However, only 2 of the 20 prohibited actions (Nos. 3 and 4) actually require damage or harm to the computer. The first (No. 3) involves the installation of a dialer,[59] and the second (No. 4) involves "using the computer as part of an activity performed by a group of computers that causes damage to another computer"—in other words, using it as part of a "bot farm."[60] The other 18 prohibited actions have no damage requirement. Although No. 9 refers to "causing damage or harm," this provision imposes a *mens rea* requirement rather than an actual damage requirement. This provision prohibits the modification of "security or other settings of the computer that protect information about the owner or authorized user *for the purposes* of causing damage or harm to the computer or owner or user."[61] In addition, No. 18 prohibits the installation of software components on another computer with the *intent* of causing a person to use such components in a way that violates any other provision of this section. The eventual use of the software may require damage to violate the Act (if used to violate Nos. 3 and 4), but violation of this section only requires intent.[62]

<21> By moving away from a regime based in part on damage or harm (whether property or dignitary) in regulating conduct between private parties, H.R. 29 substantially expands the potential scope of liability. For instance, in applying the trespass to chattels theory to the context of spyware and adware, certain types of programs just use cycle time. For instance, the damage element may be difficult to prove in cases of data miners, some Trojans, and adware, because they often will not individually impair the condition, quality, or value of a computer or deprive the possessor of its use for a substantial time. According to the logic of the California Supreme Court in *Hamidi*, damages resulting from lost time in preventing such invasions cannot be 'bootstrapped' in order to satisfy the injury requirement of the

tort because interests in time and productivity are separate from the possessory interest in the computer. As a result, many purveyors of spyware are able to operate with impunity under the trespass to chattels theory. By largely eliminating the damage element for many actions that would individually constitute negligible harm, H.R. 29 shifts the default from no liability under the trespass to chattels theory to strict liability for certain conduct.

<22> Conduct that would not currently result in liability under § 1030(a)(4)-(5) of the CFAA may also be actionable under expanded authority granted to the FTC under H.R. 29. For instance, under § 1030(a)(4), if conduct with intent to further fraud comprised only the use of the computer, $5,000 in damage related to such use must occur in any 1-year period for the government to bring an action. However, H.R. 29 prohibits "hijacking or otherwise using" the computer to "send unsolicited information from the protected computer to others."[63] No damages are required, even if this conduct was done with intent to defraud.

<23> Similarly, § 1030(a)(5)(A) prohibits the knowing transmission of information or code to a protected computer or accessing a protected computer; however, violation requires that one or more of the five factors listed in § 1030(a)(5)(B) is also satisfied: (1) damage ($5,000 in any 1-year period); (2) impairment of a medical exam; (3) physical injury; (4) a threat to public health or safety; or (5) any damage affecting a government entity in furtherance of its administration of justice, national defense, or national security. H.R. 29 appears to eliminate these factors for the range of conduct outlined in the Act, thereby imposing liability where it may not have existed before. For instance, an individual or entity "knowingly transmitting" information to a computer—such as an advertisement that the user cannot close without turning off the computer (No. 5)[64] — would not be liable under § 1030(a)(5) because it is unlikely that a factor under § 1030(a)(5)(B) would be satisfied. It would, however, be actionable by the FTC under H.R. 29. Virtually all conduct prohibited by H.R. 29 involves transmission of information or code to a protected computer or accessing a protected computer.

<24> Accessing or exceeding authorized access to *obtain information* from a protected computer under § 1030(a)(2) does not require damage; however, H.R. 29 imposes very specific requirements for securing consent/authorization to access a computer for purposes of installing an information collection program. One of the primary problems with adware and spyware is that users often give tacit consent to the installation of such programs by failing to read the fine print in EULAs or Terms of

Use agreements. Where this may constitute authorization—and therefore provide a defense to what would normally constitute a violation of § 1030(a)(2)—H.R. 29 requires *affirmative* and meaningful consent. In this respect, H.R. 29 narrows the "authorization defense," and consequentially expands the scope of liability.

<25> Finally, it is unclear how H.R. 29 will alter interpretation of Section 5 of the FTCA. Acts or practices are only "unfair" or "deceptive" if they are "*likely to cause substantial injury* to a consumer which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition."[65] The FTC carefully chooses "test" cases to guarantee a slam-dunk. In *FTC v. Seismic Entertainment Productions, Inc.*, Sanford Wallace and his affiliates sought to market anti-spyware software after installing malicious spyware on computers via a security flaw in the Internet Explorer Browser. Once a user visited a *seed* web page, a series of processes occurred almost instantaneously. Active content was used to change the user's default web page to the seed web page, which contained a script to start this process each time the user opened the browser. The seed page instructed the browser to retrieve additional pages, which could not be closed, advertising anti-spyware software. Other windows were opened containing scripts that altered the Windows registry and downloaded harmful active content without consent. These included Trojan horse programs that periodically contacted Internet hosts and allowed additional programs to be downloaded. Ads would then be sent claiming that the only way to fix the computer was to purchase Wallace's anti-spyware program.[66] A temporary injunction was issued on Oct. 21, 2004.[67]

<26> The conduct discussed herein, much of which is prohibited under H.R. 29, has led those wary of a legislative solution to argue it is unnecessary. However, what most consider to be spyware—and the software that tends to be most prolific—does not approach the devious nature involved in *Seismic*. Most such software is *adware*, which primarily tracks web surfing history, and most receive tacit consent for installation. For instance, BargainBuddy and Internet Optimizer are programs that "hijack" the browser's error page and either serve up ads or redirect the user to their websites.[68] Arguably this service does not "cause substantial injury" for purposes of violating the FTCA because the users are being directed to an actual site rather than an error page. Under H.R. 29, however, diverting the browser away from a site the user intended to view (error page or not) violates the Act, which in turn is deemed an unfair and deceptive trade practice under the FTCA despite a lack of *damage* to the computer or *injury* to the consumer.[69]

CONCLUSION

<27> The lack of a damage requirement is a relatively unique phenomenon in the current legal regime regulating private party conduct on the Internet. The actual impact it will have on bad conduct associated with spyware is unclear given the enforcement dilemmas associated with regulating conduct on the Internet.[70] No private cause of action is provided by H.R. 29, and the murky preemption regime eliminating authority of state attorneys general to bring certain actions also render the bill's impact on the spyware problem questionable at best. Nevertheless, where there is currently no legal redress for certain conduct, H.R. 29 may impose consequences.

PRACTICE POINTERS

- **Scrutinize Your Client's Notice and Consent Statements:** Consent will become the primary mechanism to prevent run-ins with the FTC. Make sure your client obtains consent in a clear notice statement pursuant to § 3 of the Act if software is used to collect a computer owner's or authorized user's information—whether it is personally identifiable information or website history.
- **Monitor the FTC's Report on Cookies:** Counsel should monitor the FTC's progress by reviewing its "Report on Cookies," which is mandated by § 8 of the SPY ACT. Section 10 of the Act exempts cookies from its definition of *computer software*, thereby preventing cookies from being subject to the Act's prohibitions. While cookies have been recognized as "innocuous and part of the basic functioning of most web sites," there is concern that more sophisticated "'tracking' or 'persistent' cookies collect identifying information and increasingly act as spyware and adware."[71] By making the distinction between *cookies* and *tracking cookies*, the SPY ACT is ambiguous as to whether the latter are subject to the Act's prohibitions or are also exempt. The report is intended to "examine and describe the methods by which such tracking cookies and the websites that place them on computers function separately and together, and the extent to which they are covered or affected by this Act."[72] The report should clarify this issue and provide insight into whether a cookie used by a client is exempt or considered a tracking cookie.

APPENDIX A: TABLE OF PROHIBITED CONDUCT UNDER H.R. 29

No.	Sec 2(a) Sub. Sec.	Shorthand Subject	Language	Consent Provides Defense to Liability	Damage Required for Violation
1	1(A) Taking Control	Spam Provision	"hijacking or otherwise using" the computer to "send unsolicited information from the protected computer to others"	No	No
2	1(B) Taking Control	Browser Diversion Provision	diverting the Internet browser away from a website the user intended to view without authorization	Yes	No
3	1(C) Taking Control	Dialer Provision	"accessing or using the modem or Internet connection or service … *and thereby causing damage to the computer* or causing the owner or authorized user or a third party defrauded by such conduct to incur charges or other costs for a service that is not authorized by such owner or authorized user"	No	Yes
4	1(D) Taking Control	Bot Farm Provision	"using the computer as part of an activity performed by a group of computers that causes damage to another computer"	No	Yes
5	1(E) Taking Control	Non-Closing Ad Windows	"delivering advertisements that a user of the computer cannot close without turning off the computer or closing all sessions of the Internet browser for the computer"	No	No
6	2(A) Modify Settings	Home Page Changing	the Web page that appears when launching a browser or "similar program used to access and navigate the Internet"	No	No
7	2(B) Modify Settings	Access/Search/Other Internet connection settings	"the default provider used to access or search the Internet, or other existing Internet connections settings"	No	No
8	2(C) Modify Settings	Bookmark Modification	"a list of bookmarks used by the computer to access Web pages"	No	No
9	2(D) Modify Settings	Modification of Security Settings	"security or other settings of the computer that protect information about the	No	No (But has mens rea

			owner or authorized user *for the purposes* of causing damage or harm to the computer or owner or user"		require.)
10	3	Keylogger Provision	"collecting *personally identifiable information* through the use of a keystroke logging function"	No	No
11	4(A) Installation or Removal	Option to Decline Installation that Really isn't an Option	"inducing the owner or authorized user to install a computer software component onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a computer software component by – (A) presenting the owner or authorized user with an option to decline installation of a software component such that, when the option is selected by the owner or authorized user or when the owner or authorized user reasonably attempts to decline the installation, the installation nevertheless proceeds"	No	No
12	4(B) Installation or Removal	Trojan Provision	"causing a computer software component that the owner or authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer"	No	No
13	5	Unneeded Software/ Unneeded Password Requirement	"misrepresenting that installing a separate software component or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate software component is necessary to open, view, or play a particular type of content"	No	No
14	6	Impersonation to Secure *Installation*	"inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user"	No	No
15	7(A)	Impersonation Secure *Information*	"inducing the owner or authorized user to provide personally identifiable, password,	No	No

			or account information to another person (A) by misrepresenting the identity of the person seeking the information"		
16	7(B)	Secure Information w/o Authority of Recipient	"inducing the owner or authorized user to provide personally identifiable, password, or account information to another person (B) without the authority of the intended recipient of the information"	Yes	No
17	8	Interfering with Defenses	"removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer"	No	No
18	9	Framing Someone Else	"installing or executing on the computer one or more additional computer software components with the *intent* of causing a person to use such components in a way that violates any other provision of this section"	Depends	Depends on Other Section
No.	**Sec 3(a) Sub. Sec.**	**Shorthand Subject**	**Language**	**Consent Provides Defense to Liability**	**Damage Required for Violation**
19	(a)(1) Unlawful To:	*Transmit* "Information Collection Program"	"…it is unlawful for any person – (1) to transmit to a protected computer, which is not owned by such person and for which such person is not an authorized user, any information collection program"	YES If 3(c) & 3(d) Satisfied	NO
20	(a)(2) Unlawful To:	*Execute* "Information Collection Program"	"… it is unlawful for any person – (2) to execute any information collection program installed on such a protected computer, *unless* (A) before execution of any of the information collection functions…"	YES If 3(c) & 3(d) Satisfied	NO
	(b)(1)	Definition of "Information Collection Program" (PII Provision)	Software that: • collects personally identifiable information and sends such information to a	N/A	N/A

			person other than the owner or authorized user of the computer; OR		
	(b)(2)	Definition of "Information Collection Program" (Adware / Webpage Monitoring)	• collects information regarding Web pages accessed using the computer AND uses such information to deliver advertising to, or display advertising on, the computer."	N/A	N/A

[<< Top]

Footnotes

1. Andrew T. Braff, University of Washington School of Law, Class of 2006, abraff@u.washington.edu. I would especially like to thank Henry L. Judy of Kirkpatrick & Lockhart Nicholson Graham LLP for his guidance on this topic.

2. Commissioners Mozelle Thompson and Orson Swindle have both opposed a legislative solution, though the FTC has not taken an official position. *See* Roy Mark, *FTC to Congress: Lose the Anti-Spyware Plans*, Internetnews.com (Nov. 5, 2004), http://www.internetnews.com/xSP/article.php/3432111 (last visited Jan. 2, 2005) (quoting FTC Commissioner Orson Swindle to Capitol Hill staffers at a Nov. 5, 2004, Cato Institute seminar; Declan McCullagh, *FTC officials blast spyware measures*, News.com (Apr. 29, 2004), http://news.com.com/2100-1023_3-5202016.html?tag=nefd.top (last visited Apr. 13, 2005)).

3. Defining the term *spyware* has been fiercely debated,

and there is no one authoritative or statutory definition. *See* A. Braff, *Defining Spyware: Necessary or Dangerous*, 2 Shidler J. L. Com. & Tech. 1 (2005), *at* http://www.lctjournal.washington.edu/Vol2/a001Braff.html (last visited Oct. 18, 2005); Joris Evers, *Group Seeks Spyware's Defining Moment*, News.com (June 3, 2005), *available at* http://news.com.com/2100-7348_3-5730290.html (last visited Mar. 5, 2006). The Anti-Spyware Coalition was formed specifically to create such a definition, and defines *spyware* as "[t]echnologies deployed without appropriate user consent and/or implemented in ways that impair user control over: (1) material changes that affect their user experience, privacy, or system security; (2) use of their system resources, including what programs are installed on their computers; and/or (3) collection, use, and distribution of their personal or other sensitive information." Anti-Spyware Coalition, Definitions and Supporting Documents, http://www.antispywarecoalition.org/documents/definitions.htm (last visited Mar. 5, 2006).

4. FTC v. Seismic Entm't Prods., Inc., Civ. No. 04-377-JD (D.N.H. Oct. 21, 2004) (order granting FTC's motion for temporary injunctive relief), *available at* http://www.cdt.org/privacy/spyware/spywiper/20041021seismicorder.
(last visited Jan. 2, 2005). For the court's rationale, *see* http://www.cdt.org/privacy/spyware/spywiper/20041021seismicruling.
(last visited Jan. 2, 2005) [hereinafter Order]. For the FTC's Complaint, and Memorandum in Support of Plaintiff's Motion for a Temporary Restraining Order *see* http://www.ftc.gov/os/caselist/0423142/0423142.htm (last visited Jan. 2, 2005) [hereinafter Memorandum].

5. H.R. Rep. No. 108-619, at 9 (2004), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:hr619.108.pdf. "The Committee does not view the technology employed by spyware and adware as the source of the problem and therefore, does not seek to regulate the software. Rather, it is the misuse of this technology that has created significant policy concerns the Committee intends to address through this legislation and ongoing oversight." *See also* A. Braff, *Defining Spyware: Necessary or Dangerous*, 2 Shidler J. L. Com. & Tech. 1 (2005), *at* http://www.lctjournal.washington.edu/Vol2/a001Braff.html

(last visited Oct. 18, 2005).

6. *Supra* note 4.

7. Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT"), H.R. 2929, 108th Cong. (2004), *at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2929rds.txt.pdf (last visited Apr. 7, 2005). H.R. 2929 passed the House of Representatives on October 5, 2004 by a vote of 399-1. 150 Cong. Rec. H8130-31 (Oct. 5, 2004), *available at* 2004 WL 2237343.

8. Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT"), H.R. 29, 109th Cong. (2005), *at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h29ih.txt.pdf (last visited Apr. 7, 2005) [hereinafter H.R. 29]. All references to the "SPY ACT," unless otherwise specified, are to H.R. 29, not H.R. 2929.

9. *See* H.R. 29, *supra* note 8. Section 4 charges the FTC with *exclusive* enforcement of violations of H.R. 29 as unfair and deceptive trade practices. Monetary penalties of up to $3 million are allowed for those engaging in a pattern or practice of violating the Act. The Act does not provide a schedule of fines for those not engaging in such violations. A single action or conduct is treated as such, even if the single action affected multiple protected computers; however, if the single action results in violations of more than one section of the Act, it is treated as multiple violations. No private cause of action is created, and Section 6 explicitly prohibits any person, other than the attorney general of a State, from bringing a "civil action under the law of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act."

10. H.R. 29 passed the House of Representatives on May 23, 2005, by a vote of 393-4. 151 Cong. Rec. H3,705-12, *available at* 2005 WL 1219039. It has been referred to the Senate Committee on Commerce, Science, and Transportation, where it remains as of this article's publication. *See also* Steptoe & Johnson LLP, *A Pre-Season Spyware Legislation Round-up*, E-Commerce Law Week (Feb. 12, 2005) *at* http://www.steptoe.com/index.cfm?fuseaction=ws.getItem&pubItemId=8943 (last visited Feb. 27, 2005). Chairman Joe Barton of the House Committee on Energy and Commerce held hearings

within a month, noting the bill is "on a fast track." Press Release, House Committee on Energy and Commerce, Committee Readies Fresh, Bipartisan Assault of Spyware (Jan. 26, 2005), *at* http://energycommerce.house.gov/108/News/01262005_1424.htm (last visited Feb. 14, 2005).

11. Federal Trade Commission Act, ch. 311, § 5, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. § 41 et. seq. (2004)).

12. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030) (hereinafter referred to as "CFAA").

13. W. P. Keeton, Prosser and Keeton on Torts, § 14 (5th ed. 1984).

14. Restatement (Second) of Torts § 218 (1965).

15. *See id*. at cmt. e.

16. Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003).

17. *Id*. at 307-8.

18. *Id*. at 308. For criticism on the use of the trespass to chattels theory in the context of computer intrusion, *see* Dan L. Burk, *The Trouble with Trespass*, 4 J. Small & Emerging Bus. L. 27 (2000).

19. 15 U.S.C. § 45(a)(1).

20. 15 U.S.C. § 45(n) (emphasis added).

21. Press Release, Federal Trade Commission, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* http://www.ftc.gov/opa/2002/01/elililly.htm (last visited Mar. 26, 2005); Press Release, Federal Trade Commission, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), *available at* http://www.ftc.gov/opa/2002/08/microsoft.htm (last visited Mar. 26, 2005); Press Release, Federal Trade Commission, Guess Settles FTC Security Charges; Third FTC Case Targets False Claims About Information Security (June 18, 2003), *available at* http://www.ftc.gov/opa/2003/06/guess.htm (last visited Mar. 26, 2005); Press Release, Federal Trade Commission, Tower Records Settles FTC Charges (Apr. 21, 2004), *available at* http://www.ftc.gov/opa/2004/04/towerrecords.htm

(last visited Mar. 26, 2005).

22. *See* Memorandum, *supra* note 4, at 1.

23. No. 00-CV-32 (D.D.C. Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm (last visited 04/05/05). ReverseAuction.com, Inc., was charged with improperly obtaining personal information from eBay customers and using it to spam them with competing promotions in violation of § 5 of the FTCA. Though the Commissioners voted 5-0 to approve the settlement, they disagreed on the interpretation of "substantial injury." *See* Stipulated Consent Agreement and Final Order, *available at* http://www.ftc.gov/os/2000/01/reverseconsent.htm, Stmt. of Comm'rs Orson Swindle & Thomas B. Leary, FTC File No. 002-3046, *available at* http://www.ftc.gov/os/2000/01/reversesl.htm, and Stmt. of Comm'r Mozelle W. Thompson, FTC File No. 002-3046, *available at* http://www.ftc.gov/os/2000/01/reversemt.htm (last visited Apr. 5, 2005).

24. S. Rep. No. 104-357, pt. II (1996), *available at* 1996 WL 492169.

25. Provisions of the CFAA pertaining specifically to government computers are 18 U.S.C. §§ 1030(a)(1), (a)(2)(B), (a)(3), (a)(5)(B)(v), and (a)(6). Section 1030(a)(1) prohibits knowingly accessing "a computer without authorization, or exceeding authorized access," and essentially obtaining information deemed classified or otherwise protected either by executive order or statute. Section 1030(a)(2)(B) is broader and prohibits intentionally accessing a computer without authorization, or exceeding authorized access, and thereby obtaining information from any department or agency of the United States. Section 1030(a)(3) similarly prohibits intentionally accessing, "without authorization, any nonpublic computer of a department or agency of the United States." In the "case of a computer not exclusively for such use," this section also prohibits accessing a computer in such a manner that "affects that use by or for the Government of the United States." Section 1030(a)(5)(B)(v) prohibits damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. To violate this particular subsection, the perpetrator must knowingly cause the transmission of a program, information, code, or

command resulting in damage to a "protected computer," intentionally access a protected computer and recklessly cause damage, or simply intentionally access a protected computer without authorization and cause damage to the computer. The CFAA also contains separate provisions for accessing computers used by financial institutions or those regulated by the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. Only provisions that potentially encompass all private computers are discussed given the specific nature of the provisions relating to heavily regulated industries.

26. Pub. L. No. 98-473, 98 Stat. 2190 (1984).

27. In 1986, Congress closed this loophole by including the phrase "or exceeds authorized access." Pub. L. No. 99-474, § 2(c), 100 Stat. 1213 (1986).

28. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, § 290,001(d), 108 Stat. 1796, 2098 (1994).

29. *See* 139 Cong. Rec. S16,421-03 (daily ed. Nov. 19, 1993) (statement of Sen. Leahy).

30. Pub. L. No. 104-294, § 201(4)(A)(i), 110 Stat. 3488, 3493 (1996).

31. 18 U.S.C. 1030(e)(2)(B). Section 1030(e)(2)(A) also defines "protected computer" as a computer "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government."

32. *Id*.

33. 18 U.S.C. § 1030(a)(2)(c) (emphasis added).

34. "Bundling," the practice of combining a number of related or unrelated programs in a single installation, has increased as a way to disseminate software in mass quantities, achieve exposure, and reduce costs for the consumer. This arrangement poses complications for resolving the spyware problem because the user provides "consent" when downloading the programs. This consent, however, is questionably meaningful because of the growing length of end user license agreements and the corresponding likelihood that the user does not know what exactly is being downloaded. Ari Schwartz, Remarks, *Monitoring Software on Your PC: Spyware, Adware, and Other Software*, FTC Public Workshop, at

45 (Apr. 19, 2004), *available at* http://www.ftc.gov/bcp/workshops/spyware/ (last visited Jan. 2, 2005).

35. 15 U.S.C. § 45.

36. 18 U.S.C. § 1030(a)(4).

37. *Id. See United States v. Czubinski,* 106 F.3d 1069, 1078 (1st Cir. 1997) (defendant employee of IRS's Taxpayer Services Division did not violate the CFAA when he exceeded his authorized access by using his password to review tax returns of his friends and enemies because he obtained a mere satisfaction of his curiosity, which did not constitute "anything of value.").

38. 18 U.S.C. § 1030(a)(4).

39. 18 U.S.C. § 1030(a)(5).

40. 18 U.S.C. § 1030(e)(8).

41. Recently expanded, the definition of "loss" appears to have a broader meaning under the CFAA than "damage" does under the trespass to chattels theory as outlined in *Hamidi*. Under the CFAA, "loss" is now defined as any "reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 814(d), 115 Stat 272, 384 (2001) (amending § 1030(e)), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf (last visited Apr. 7, 2005).

42. 18 U.S.C. § 1030(g).

43. CAN-SPAM Act of 2003, Pub. L. No. 108-187, § 4(a), 117 Stat. 2699, 2703-06 (2003) (codified at 18 U.S.C. § 1037 and 15 U.S.C. § 7701 et seq.), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf (last visited Apr. 7, 2005).

44. As with spyware, there is debate over exactly to define *Spam.* The term is generally used to refer to the action of indiscriminately sending unsolicited, unwanted, irrelevant, or inappropriate electronic

messages, particularly commercial advertising, in mass quantities. *Spam* is also used as a noun to refer to the actual email bearing such characteristics.

45. 18 U.S.C. § 1037(b)(2)(D).

46. In the context of spyware, a *dialer* is a program that changes a user's dialup connection setting so instead of calling a local Internet service provider (ISP), the modem dials an expensive "1-900" number or international phone number.

47. A *Trojan* is defined as "a software program that enables an attacker to get nearly complete control over an infected PC. … When this program executes, the program performs a specific set of actions, usually working toward the goal of allowing the Trojan to survive on a system" and open up a "backdoor" allowing continual exploitation of the computer. *See* Spywareguide.com, http://www.spywareguide.com/category_show.php?id=1 (last visited March 5, 2006).

48. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

49. Cookies are bits of information sent by a web server and stored on a user's computer, enabling the visited website to customize material and recall preferences if visited in the future. *See* Dictionary.com *available at* http://dictionary.reference.com/search?q=cookie (last visited Sept. 12, 2005). H.R. 29 distinguishes between "cookies" and "tracking cookies." In exempting cookies from the definition of *computer software*, cookies are protected from classification as spyware. A *cookie* is categorized generally as a "(i) … text or data file that is placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet website to return information to such provider, service or website; or (ii) computer software that is placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet website solely to enable the user subsequently to use such provider or service to access such website." H.R. 29, *supra* note 8, § 10(4)(B). The term *tracking cookie* is specifically defined as "a cookie or similar text or data file used alone or in conjunction with one or more websites to transmit or convey personally identifiable information regarding Web pages accessed by the owner or user, to a party other than the intended recipient, for the purpose of:

(1) delivering or displaying advertising to the owner or user; or (2) assisting the intended recipient to deliver or display advertising to the owner, user or others." H.R. 29, *supra* note 8, § 8(b).

50. 18 U.S.C. § 2701(c) (2004).

51. *In re* DoubleClick, 154 F. Supp. 2d at 507, 513-14.

52. 18 U.S.C. § 2511.

53. H.R. 29, *supra* note 8, § 3(b).

54. *Id*. at § 3(c)(2)-(3).

55. *Id*. at § 3(d)(1)-(2). An amendment was adopted allowing the FTC to exempt "embedded advertisements" from the "identity requirement." The term "embedded advertisements" is not defined.

56. *Id*. at § 5.

57. *Id*. at § 6.

58. 18 U.S.C. § 1030(e)(8).

59. H.R. 29, *supra* note 8, § 2(a)(1)(C). For a definition of *dialer*, see note 46, *supra*.

60. *Id*. at § 2(a)(1)(D).

61. *Id*. at § 2(a)(2)(D).

62. *Id*. at § 2(a)(9).

63. *Id.* at § 2(a)(1)(A).

64. *Id.* at § 2(a)(1)(E).

65. 15 U.S.C. § 45(n) (emphasis added).

66. Declaration of Steven D. Gribble, *FTC v. Seismic Entm't Prods., Inc.*, Civ. No. 04-377-JD (D.N.H. 2004).

67. *See* FTC v. Seismic Entm't Prods., Inc., Civ. No. 04-377-JD (D.N.H. Oct. 21, 2004) (order granting FTC's motion for temporary injunctive relief), *available at* http://www.cdt.org/privacy/spyware/spywiper/20041021seismicorder.
(last visited Jan. 2, 2005).

68. For more information see "BargainBuddy", SpywareGuide, *at* http://www.spywareguide.com/product_show.php?id=463 (last visited Feb. 28, 2005); "Internet-Optimizer," SpywareGuide, *at* http://www.spywareguide.com/product_show.php?id=869 (last visited Feb. 28, 2005).

69. H.R. 29, *supra* note 8, § 2(a)(1)(B).

70. H.R. Rep. No. 108-619, *supra* note 5, at 12. The Congressional Budget Office predicts enforcement would generate approximately $500,000 in revenue for the government and spending by the FTC on enforcement to be "insignificant." This suggests enforcement of the law is intended to be minimal and will likely prove inadequate to quell the proliferation of spyware.

71. H..R. Rep. No. 109-32, at 22 (2005), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr032.109.pdf (last visited Oct. 15, 2005).

72. H.R. 29, *supra* note 8, § 8(a).

<< Top