JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.1 (2013)

Got Cookies?

Bose v. Interclick, Inc.: Computer Fraud and Abuse Act Claims Dismissed With Prejudice Due To Lack of Precedent Providing for the Value of Personal Information and an Unclear Standard for Aggregation of Damages

Samantha C. Arrington

North Carolina Central University School of Law
arringtonsc@yahoo.com

Abstract: In *Bose v. Interclick, Inc.*, a federal district court judge in New York dismissed Bose's claim under the CFAA because she did not meet the statutory requirement under the statute. Bose is one of many CFAA claim dismissals in the United States where the federal district court refused to hear the case because the plaintiff failed to meet the statutory damages requirement but recognized that the plaintiff had suffered an injury. This note focuses on the negative effects of CFAA claim dismissals on plaintiffs, the need for federal courts to decide the value of personal information, and the appropriate formula for the aggregation of damages. It is imperative that defendants in violation of the CFAA be punished for stealing personal information from innocent Internet users. The United States legal system is an active member of the fast paced, technological era that is currently unfolding, and it is important for our legal system to recognize and combat illegal behavior on the part of Internet advertising companies that steal personal information from unsuspecting, unknowing Internet users. If not, this epidemic will continue and expand into other types of personal information regarding a person's health, etc. First, this note provides a factual summary of *Bose v. Interclick, Inc.*, and the court's basis for the dismissal of the CFAA claim. Secondly, this note provides a background of the CFAA and the case law governing CFAA claims in federal court. Next, this note provides an analysis of the importance of establishing the value of personal information and developing a standardized method to determine aggregation of damages. Lastly, this note provides a conclusion detailing an overview of the key points of discussion.

1. Introduction

Have you ever wondered how Facebook seems to know exactly what merchandise you would be willing to purchase by placing your favorite items in advertisements on their website? Technically, you can think advertising companies, like Interclick, for these ads. Facebook and other websites contract with advertising companies so that the most influential ads will appear on their websites and increase business for partnering companies.

With every click of the mouse and every webpage you visit your personal information including credit card numbers, social security numbers, passwords, and medical records, have the potential to be accessed by third parties without your permission. Nielsen and the Pew Research Center found that "55 percent of Americans use the Internet every day" and devote "60 hours a month online."[1] "The world spends 36 percent of its web time using e-mail, engaging in commerce, or performing web searches;" "42 percent of this time is spent viewing content."[2] "In a single month, a web user visits 2,646 sites and logs on 57 times."[3] These statistics show that most Americans would be subject to these types of intrusions.

The unsolicited seizure and use of personal information acquired via the Internet affects all Internet users. The Computer Fraud and Abuse Act (CFAA) was enacted to provide criminal liability and a civil cause of action for persons affected by computer fraud and abuse.[4] However, the case law demonstrates

[1] Catherine Smith, *Internet Usage Statistics: How We Spend Our Time Online (Infographic)*, Huffington Post, (June 22, 2010), http://www.huffingtonpost.com/2010/06/22/internet-usage-statistics_n_620946.html.
[2] *Id.*
[3] *Id.*
[4] 18 U.S.C. § 1030 (2011).

that it is extremely difficult for an individual or class of individuals to successfully bring a civil claim under the CFAA.

Why are civil claims so difficult to plead? In order to bring a claim under the CFAA, a person(s) must suffer compensatory damages in the aggregate of $5000.00.[5] This limit is often hard to meet because the loss incurred is most often the loss of personal information. No federal court has determined the dollar value of personal information or designated a method for calculating its value; therefore, many plaintiffs are hard-pressed to plead a damages amount that will meet the requisite $5000.00 threshold. Additionally, most plaintiffs cannot reach the aggregate limit alone; therefore, a class action is pursued so that individuals suffering the same injury or damages can satisfy the statutory requirement as a class. This creates yet another problem. The federal district courts are split as to how damages can be aggregated under the CFAA.[6]

In *Bose v. Interclick, Inc.*, a federal district court judge in New York dismissed Bose's claim under the CFAA because she did not meet the statutory requirement under the statute.[7] *Bose* is one of many CFAA claim dismissals in the United States where the federal district court refused to hear the case because the plaintiff failed to meet the statutory damages requirement but recognized that the plaintiff had suffered an injury.

This note focuses on the negative effects of CFAA claim dismissals on plaintiffs, the need for federal courts to decide the value of personal information and the appropriate formula for the aggregation of damages. It is imperative that defendants in violation of the CFAA be punished for stealing personal information from innocent Internet users. The United States legal system is an active member of the fast paced, technological era that is currently unfolding, and it is important for our legal system to recognize and combat illegal behavior on the part of Internet advertising companies that steal personal information from unsuspecting, unknowing Internet users. If not, this epidemic will continue and expand into other types of personal information regarding a person's health, etc.

First, this note provides a factual summary of *Bose v. Interclick, Inc.*, and the court's basis for the dismissal of the CFAA claim. Secondly, this note provides a background of the CFAA and the case law governing CFAA claims in federal court. Next, this note provides an analysis of the importance of establishing the value of personal information and developing a standardized method to determine aggregation of damages. Lastly, this note provides a conclusion detailing an overview of the key points of discussion.

2. The Case

On December 8, 2010, Sonal Bose, brought a class action suit against Interclick, Inc., an advertising network company, under Computer Fraud and Abuse Act.[8] On December 23, 2010, Bose also filed suit against the advertisers, "McDonald's USA LLC, McDonald's Corp., CBS Corp., Mazda Motor Corp. of America, Inc. Microsoft Corp., and Does 1-50."[9] These cases were consolidated with the filing of an amended complaint on March 21, 2011.[10] On April 18, 2011, all defendants filed motions to dismiss on the grounds that Bose failed "to allege a cognizable injury or meet the $5000.00 damages threshold to state a claim under the CFAA."[11]

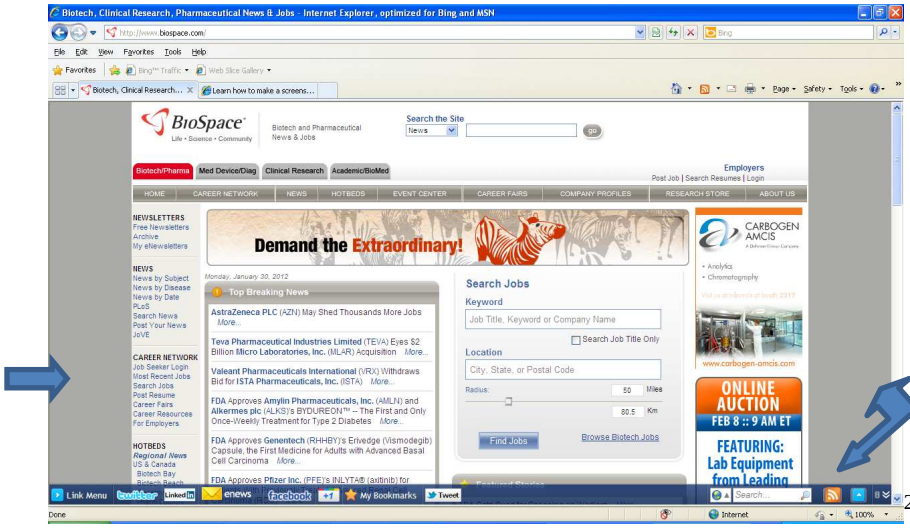
Bose, a frequent Internet user, reviewed the contents of her local storage associated with the Adobe Flash Player[12] application on her computer in late October 2010.[13] During the review, Bose discovered a

---

[5] *See id.* § 1030(e)(8)(A).
[6] *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y.,2001), *see also In re Toys R Us Inc. Privacy Litigation*, No. 00 Civ. 2746, 2001 WL 34517252 (N.D.Cal. Oct. 9, 2001).
[7] *Bose v. Interclick, Inc.*, No. 10-Civ-9183 (S.D.N.Y. Aug. 17, 2011) (order granting motion to dismiss), *available at* http://www.scribd.com/doc/62531370/Bose-v-Interclick.
[8] *Id*.
[9] *Id*.
[10] *Id*. at 4.
[11] *Id*. at 1.
[12] *About Updating Flash* Player, MACROMEDIA.COM, http://www.macromedia.com/support/documentation/en/flashplayer/help/help10.html (last visited Jan. 6, 2012) ("Adobe Flash Player is software created by Adobe that lets a user view interactive content and applications on the web").

Local Shared Object (LSO) placed on her computer by interclick.com."[14] Interclick is an advertising company that purchases advertisement display space from websites, and displays advertisements to an Internet user that would interest them based on their browsing history.[15] Advertising companies and agencies hire Interclick to display their advertisements on websites within Interclick's advertising network.[16]

"For the month of December 2009, comScore Media Metrix[17] ranked Interclick 10th among U.S. Internet advertising networks, with an audience of approximately 149 million unique users, over 72 percent of the total Internet audience that month."[18] When a third-party advertisement is displayed to an Internet user, the spawning of particular advertisements is caused by the web page communicating with the ad network's systems.[19] These advertisements can range from pharmaceutical companies advertising clinical trials and new medications to Trident advertising its latest flavor of gum. Thus, consumers that become a part of Interclick's "audience" may not even know of their interaction with or communication with Interclick because inclusion in the "audience" is based upon the accessing of websites on which Interclick displayed its clients' advertisements.[20] Interclick's advertising network consists of websites, also known as publishers, which Interclick pays to make use of.[21] These publishers make up Interclick's advertising inventory[22].[23]



[24]

When Interclick pays to expend the advertising space on a website, this is remnant inventory[25], also called 'non-premium' inventory."[26] When Interclick is hired by an advertiser, the advertiser pays based

---

[13] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 14, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20.
[14] *Id.*
[15] *Bose*, at 2.
[16] *Id.*
[17] *About comScore*, COMSCORE.COM, http://www.comscore.com/About_comScore (last visited Jan. 6, 2012) ("comScore is a global leader in measuring the digital world and the preferred source of digital marketing intelligence. Through a powerful combination of behavioral and survey insights, comScore enables clients to better understand, leverage and profit from the rapidly evolving worldwide web and mobile arena. comScore provides syndicated and custom solutions in online audience measurement, e-commerce, advertising, search, video and mobile and offers dedicated analysts with digital marketing and vertical-specific industry expertise. Advertising agencies, publishers, marketers and financial analysts turn to comScore for the industry-leading solutions needed to craft successful digital, marketing, sales, product development and trading strategies").
[18] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 5, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.* ("Inventory is advertising display space on web pages").
[23] *Id.*
[24] BIOSPACE, www.biospace.com/ (last visited Feb. 28, 2012).

on the type of inventory being used to display their advertisements.[27] Fees for premium inventory usually are based on cost per thousand ad views (CPMs), while ads distributed on remnant inventory are based on performance-based fees.[28] How an Internet user reacts to an advertisement, such as mousing over, clicking on, or clicking through an advertisement, will affect the amount of the performance-based fees paid to Interclick.[29] The bulk of Interclick's revenue is based on performance-based fees.[30]

Many advertising companies, including Interclick, use text files that gather information about a computer user's Internet habits called "browser cookies."[31] "Browser cookies contain unique identifiers and associate browsing history information with particular computers."[32] Advertising companies create behavioral profiles from the browsing history stored on computers by the browser cookies.[33] These behavioral profiles assist the advertising company in selecting particular advertisements to be displayed to individual Internet users.[34] Behavioral profiles allow Interclick to maximize "return on ad spend" by targeting specific users for the advertisements that will most likely result in the user performing some function with the advertisement.[35]

Here, "Bose alleged that Interclick used "flash cookies" or LSOs to back up browser cookies."[36] Normally, an Internet user can delete or block browser cookies to prevent third parties from accessing their browsing history information.[37] However, when an Internet user deletes a browser cookie, a flash cookie recreates the browser cookie without notice to or consent of the user.[38] The University of California, Berkeley performed a study, "Flash Cookies and Privacy," that confirmed Interclick's use of this technology.[39] Researchers discovered that a user visiting an Interclick website received not only a standard browser cookie, but also a flash cookie.[40] The placement of the flash cookie was unknown to the user, and the "respawning" of the browsing history occurred without any consent from the user.[41]

"Flash cookies are files designed to be used by consumers' Adobe Flash Player software[42], for purposes such as storing a consumer's volume control preference for audio content or retaining the score of a video game the consumer plays in multiple sessions."[43] Adobe Systems Incorporated stated in a letter the Federal Trade Commission that, "Adobe condemns the practice of using Local Storage to back up browser cookies for the purpose of restoring them later without user knowledge and express consent."[44] Here, Bose alleged that "Interclick stored LSOs on consumers' computers for purposes other

---

[25] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 5, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20. ("After websites sell their premium inventory, which they typically sell directly to advertisers, with guarantees regarding factors such as ad placement, times of day, and volume of traffic, the remaining, unsold inventory is remnant inventory").
[26] *Id*.
[27] *Id*.
[28] *Id*.
[29] *Id*. at 6.
[30] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 6, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20.
[31] *Bose*, at 2-3.
[32] *Id*. at 3.
[33] *Id*.
[34] *Id*.
[35] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 6, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20.
[36] *Bose*, at 3.
[37] *Id*.
[38] *Id*.
[39] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 7, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20. *See also*, Ashkan Soltani, Shannon Canty, Quenton Mayo, Lauren Thomas & Chris .J. Hoofnagle, *Flash Cookies and Privacy*, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.
[40] *Id*. *See also*, Ashkan Soltani, Shannon Canty, Quenton Mayo, Lauren Thomas & Chris .J. Hoofnagle, *Flash Cookies and Privacy*, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.
[41] *Id*. at 8. *See also*, Ashkan Soltani, Shannon Canty, Quenton Mayo, Lauren Thomas & Chris .J. Hoofnagle, *Flash Cookies and Privacy*, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.
[42] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 7, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20 ("Adobe Flash Player is installed on the majority of U.S. consumers' computers").
[43] *Id*.
[44] Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf.

than delivering content to play on consumers' Flash Players or to retain settings for playing Flash content chosen by consumers."[45]

"Interclick reportedly claims to no longer uses LSOs for ad targeting."[46] However, flash cookies previously placed on a user's computer linger on the computer for Interclick to employ."[47] There are no reasonable resources available to Internet users to detect or delete the flash cookies.[48] Internet users are generally not aware of the tool presently offered by Adobe for controlling flash cookies, and Internet users commonly do not recognize a need for this tool.[49] Notwithstanding the Adobe protection mechanism, Internet users should not be held liable to protect themselves from intrusions by Interclick and like companies, when absent the conduct of these companies the need for protection would be nonexistent.[50]

Bose also alleged that "Interclick used invisible 'history sniffing[51]' code."[52] Bose contended that "Interclick performed history-sniffing as follows: (a) in its code to display an advertisement to a consumer, Interclick embedded history-sniffing code invisible to the consumer; (b) the history-sniffing code contained a list of web page hyperlinks; (c) although the hyperlinks were not displayed to the consumer, the consumer's browser automatically assigned each link a color designation based on whether the user had previously visited the web page associated with the link; (d) the history-sniffing code performed an examination of the list of color-designated hyperlinks; and (e) the history-sniffing code transmitted the results of this examination to Interclick's servers."[53]

Interclick's history sniffing attack chronicles an Internet user's browsing history of the Interclick website along with other websites the user visits.[54] This technique was used to assist Interclick in constructing behavioral profiles and selecting appropriate advertisements to be displayed to particular Internet users."[55] Cross-domain activity such as history sniffing violates global Internet standards.[56]

A report authored by the University of California, San Diego exposed Interclick's use of history sniffing, and indicated that Interclick was most commonly connected with this practice.[57] The report revealed that "the web pages on which Interclick performed browser-history sniffing, Interclick's hidden list of hyperlinks contained links for as many 222 websites."[58]

The United States District Court for the Southern District of New York, Judge Deborah A. Batts, held that Bose's amended complaint must be dismissed with prejudiced because she failed to assert personal economic loss under the CFAA.[59] The court found that "Bose failed to quantify any damage that Interclick caused to her computers, systems or data that could require economic remedy."[60] "Bose's allegations concerning 'invasion of [her] privacy', 'trespass,' and 'misappropriation of confidential data' were also found not to be cognizable injuries."[61] "Bose also failed to allege specific damage or loss incurred due to alleged interruption of service, or costs incurred to remedy the alleged interruption of

---

[45] Amended Complaint and Demand for Jury Trial, *Bose v. Interclick, Inc.* at 7, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20 ("Adobe Flash Player is installed on the majority of U.S. consumers' computers").
[46] *Id*. at 8.
[47] *Id*.
[48] *Id*.
[49] *Id*.
[50] *Id*.
[51] *Id*. ("History sniffing exploits the standard browser function that causes a user's previously visited links to be displayed in a different color than links a user has not visited").
[52] *Bose*, at 3.
[53] Amended Complaint and Demand for Jury Trial, *Bosh v. Interclick, Inc*. at 9, No 10- Civ-9183 (S.D.N.Y. March 21, 2011), ECF No. 20 ("Adobe Flash Player is installed on the majority of U.S. consumers' computers").
[54] *Id*. (This technique of acquiring consumers' web activity data is known as "browser history sniffing" or a "history-sniffing attack").
[55] *Id*.
[56] *Id*.
[57] *Id*. 9-10, *See also*, Dongseok Jang, Ranjit Jhala, Sorin Lerner & Hovav Shacham , *An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications*, Univ. Cal., San Diego, (Oct. 2010), sec. 4, http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf .
[58] *Id*. at 10. *See also*, Dongseok Jang, Ranjit Jhala, Sorin Lerner & Hovav Shacham , *An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications*, Univ. Cal., San Diego, (Oct. 2010), sec. 4, http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf .
[59] *Bose*, at 17.
[60] *Id*. at 10.
[61] *Id*. at 11.

service."[62] On the matter of aggregation, the court recognized that "the Second Circuit Court of Appeals had not yet addressed whether losses could be aggregated for purposes of the CFAA before a class is certified, but the Second Circuit had indicated approval of *In Re DoubleClick's* thorough exploration of the CFAA."[63]

3. Background

To facilitate a thorough comprehension of the factual summary and the analytical argument that follows, it is imperative to understand the CFAA as it was applied in Bose.

3.1 Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act 1986 was enacted by Congress to prohibit unauthorized access to broad classes of computerized data.[64] Information from any department or agency of the United States[65], and any "protected" computer if the conduct involved an interstate or foreign communication is protected under the statute.[66] A "protected computer" includes computers used by financial institutions, the United States government, or any computer "used in interstate or foreign commerce or communication."[67] The statute further provides that one who intentionally accesses a protected computer without authorization or exceeds authorized access, and thereby obtains certain types of; or who intentionally accesses a protected computer without authorization, and thereby causes damage, is subject to fine or imprisonment.[68] The civil enforcement provision of the CFAA provides: "any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[69]

3.2 Aggregation of Damages

There are two separate sections concerning damages in the Computer Fraud and Abuse Act. 18 U.S.C. § 1030(e)(8) (2011) provides that the term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information."70 18 U.S.C. § 1030(e)(11) (2011) defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the date, 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."[71] In addition, 18 U.S.C. 1030(g) (2011) provides, in relevant part, that:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in section (e)(8)(A) are limited to economic damages."[72]

---

[62] *Id*. at 14.
[63] *Id*. at 15 ("*In Re Doubleclick*, the court concluded that damage and loss may only be aggregated across victims and over time for a single act." 154 F. Supp. 2d 497, 523 (S.D.N.Y.,2001) (declining to aggregate claims that defendant placed cookies on multiple computers and noting that the CFAA defines damage in § 1030(e)(8) in the singular form, "any impairment to the integrity or availability of data, a program, a system, or information," rather than the plural form, "any impairments to the integrity or availability of data, programs, systems, or information"); *see also* S. Rep. No. 99-132, at 5 (1986) (explaining that loss caused by the "same act" can be aggregated to meet the $5000.00 threshold).
[64] 18 U.S.C. § 1030 (2011).
[65] *See id*. § 1030(a)(2)(B).
[66] *See id.* § 1030(a)(2)(C).
[67] *See id.* § 1030(e)(2)(B).
[68] *See id.* § 1030(c).
[69] *See id*. § 1030(g).
[70] *See id*. § 1030(e)(8).
[71] *See id*. § 1030(e)(11).
[72] *See id*. § 1030(g).

The subsection referred to in section (g) establishes the $5,000.00 threshold for "damage."[73] Thus, "the question arises as to whether the term "damage or loss" is necessarily limited by the $5,000.00 threshold stated in the statute."[74]

Plaintiffs in *In re DoubleClick Inc. Privacy Litigation* argued that the $5000.00 "damage" threshold was not applicable in the case because "loss" under the statute was distinct from "damage".[75] In contrast, plaintiffs argued that if the damage threshold was found applicable to plaintiffs' claims, the class could aggregate its losses over a 1-year period and satisfy the damages threshold.[76] The court held that the plaintiffs' alleged injuries were subject to the $5000.00 statutory threshold, regardless of whether the damages were described as "damages" or "losses."[77] The court further found that "damages may only be aggregated across victims and over time for a single act."[78] The court concluded that plaintiffs failed to plead facts that could support a finding that any single act by DoubleClick resulted in plaintiffs suffering over $5000.00 in damages and/or losses.[79]

The *In re DoubleClick Inc. Privacy Litigation* court articulated the definition of a prohibited act as revolving around a "perpetrator's access to a particular computer."[80] A very persuasive passage by Judge Buchwald stated:

> The prohibition is phrased in the singular: [whoever] intentionally accesses a computer without authorization . . . and thereby obtains . . . (C) information from any protected computer . . . Thus, the suggestion that DoubleClick's accessing of cookies on millions of plaintiffs' computers could constitute a single act is refuted by the statute's plain language.[81]

The court noted that it could be argued that DoubleClick committed a violation of the Act each time it retrieved a cookie on a plaintiff's hard drive.[82] Additionally, albeit the automatic uploading of information from a cookie ensues over numerous electronic transactions, it is believed to be a single act of "access" by the court.[83] The district court did not need to distinguish between the two interpretations in *In re DoubleClick Inc. Privacy Litigation* because plaintiffs failed to plead facts that satisfied the damages threshold under either interpretation.[84]

"Some courts in the Ninth Circuit have concluded that damages can be aggregated across multiple computers."[85] "Certain types of malicious mischief may cause smaller amounts of damage to numerous individuals, and thereby collectively create a loss of more than $1,000.00." reasoned the court in *In re Toys R Us Inc. Privacy Litigation*.[86] The court concluded that because the committee referred to "numerous individuals," damages across multiple computers could be aggregated.[87] Under this aggregation method, multiple intrusions across a one-year period can cause a single impairment to data, and the statute does not limit impairment to the result of a single intrusion or a single corrupted byte.[88]

---

[73] 67 AM. JUR. PROOF OF FACTS 3D 249 § 16 (2002).
[74] *Id*.
[75] *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 520.
[76] *Id*.
[77] *Id*. at 523.
[78] *Id*.
[79] *Id*. at 524.
[80] *Id*.
[81] *Id*.
[82] *Id*.
[83] *Id*.
[84] *Id*.
[85] *Bose*, at 16.
[86] *In re Toys R Us Inc. Privacy Litigation*, No. 00 Civ. 2746, 2001 WL 34517252, at *11 n.20 (N.D.Cal. Oct. 9, 2001) (quoting Sen. Rep. No. 99-132).
[87] *Id*. (holding that when "Defendants caused an identical file to be implanted in each of the Plaintiffs' computers, resulting in damages of a uniform nature," Plaintiffs could aggregate "damages exceeding $5,000.00 during any one-year period to one or more individuals").
[88] *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934-35 (9th Cir. 2004).

3.3 Economic Damages

Plaintiffs in *In re DoubleClick* claimed they had been defrauded out of the value of 1) the opportunity to present plaintiffs with advertising and 2) the demographic information DoubleClick had collected; thus, plaintiffs suffered economic damages.[89] Plaintiffs contended "that because companies pay DoubleClick for plaintiffs' attention to advertisements and demographic information, the value of these services must, in some part, have rightfully belonged to plaintiffs."[90]

The court held that it did not "believe that the economic value of our attention is unjustly taken from us when we choose to watch a television show or read a newspaper with advertisements, and that there is not any statute or case law that holds it is."[91] Based on this reasoning, the court could unearth no reason why Internet advertising should be treated any differently than other methods of advertising.[92] An Internet user is no more denied of the economic value of their attention than other off-line individuals because the user chooses to view particular websites, and thus consents to the possibility of being faced with a targeted advertisement.[93]

No court has ever deemed the economic value of demographic information to be a loss to the individual when it is collected by third parties or an unjust enrichment to third party collectors, even though sources show that demographic information is valued highly by third parties such as DoubleClick.[94] The value of demographic information is evidenced by DoubleClick's over one billion dollars acquisition of Abacus Direct[95].[96] It appeared to the court that "plaintiffs failed to state any facts that could supported a finding of economic loss from DoubleClick's alleged violation of the CFAA."[97]

Correspondingly, in *LaCourt v. Specific Media, Inc.*, the United States District Court for the Central District of California dismissed a CFAA claim by plaintiffs who alleged that they set privacy and security controls on their computers to block and delete third party cookies.[98] The plaintiffs also argued that "the defendant had flash cookies installed on plaintiffs' computers without notice or consent."[99] Finding that plaintiffs had failed to allege economic injury, the court noted,

> The Complaint does not identify a single individual who was foreclosed from entering into a "value-for-value exchange" as a result of Specific Media's alleged conduct. Furthermore, there are no facts that indicate that the Plaintiffs themselves ascribed an economic value to their unspecified personal information. Finally, even assuming an opportunity to engage in a "value-for-value exchange," Plaintiffs do not explain how they were "deprived" of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party.100

---

[89] *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 525.
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 525. *See also*, *Civic Ctr. Motors, Ltd. V. Mason St. Imp. Cars, Ltd.*, 387 F. Supp.2d 378, 382 (S.D.N.Y. 2005) (holding that lost profits from defendant's unfair competitive edge were not economic damages under the CFAA).
[95] *Abacus Direct Corporation*, BLOOMBERG BUSINESSWEEK, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=24157 (last visited Jan. 6, 2012) ("Abacus Direct Corporation operates as a data and research provider to the direct marketing industry. The company manages the proprietary transactional database of behavioral data from catalog, retail, business to business, e-commerce, and publishing markets. In addition, Abacus offers multichannel marketing solutions, which include an analysis tool to help users determine the ROI of an email or direct marketing campaign across the user's Web, retail stores, and catalog call centers").
[96] *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 525.
[97] *Id.*
[98] *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256-GW(JCGx), 2011 WL 1661532, at *1 (C.D.Cal. April 28, 2011).
[99] *Id.*
[100] *Id.* at *5.

The Court then held that a plaintiff's inability to delete or control cookies may constitute de minimis injury, but such injury was still insufficient to meet the $5,000.00 threshold.[101] The *LaCourt* court concluded that:

> While Plaintiffs attempt to distinguish *DoubleClick* on the ground they have alleged that they were deprived not of "mere demographic information," but "of the value of their personal data," it is not clear what they mean by this. Defendant observes that, if anything, the Plaintiffs in *DoubleClick* alleged that the defendant collected much more information than Specific Media supposedly collected in this case, including "names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect."

4. Analysis

The CFAA was enacted to prohibit unauthorized access of broad classes of computerized data.[102] Historically, the courts have erred by dismissing CFAA claims because the unauthorized access of personal information through flash cookies and history sniffing has been determined to be a de minimis injury to plaintiffs. The courts are making a huge mistake by dismissing the claims of plaintiffs that have suffered a detrimental loss. Plaintiffs should be able to recover for the damages and losses they incur because of the theft of their personal information. The unauthorized access of a person's personal information is exactly what the CFAA was designed to combat. By allowing violators to commit these illegal acts with no repercussions, the courts are facilitating and increasing the presence of these illegal acts by advertising companies.

Federal courts in New York and California have both held that demographic and personal information stolen by advertising companies on the Internet through deceptive practices such as, history sniffing, has no economic value to the victim.[103] However, while the *In re DoubleClick* court ruled in the alternative, the court did recognize that demographic information is highly valued by advertising networks.[104] The high value of demographic information is evidenced by transactions such as the merger of DoubleClick and Abacus Direct.[105] During this merger, DoubleClick paid over one billion dollars for the market research company Abacus Direct.[106] It is obvious that personal information has a high value, not only to the person that it rightfully belongs to, but to advertising networks such as DoubleClick, Interclick and Specific Media. These companies spend millions of dollars to purchase personal information from market research companies so that they can better tailor their online advertisements to the specific viewers their clients are wanting to reach; thus, resulting in a higher profit for their company.

Furthermore, social networking sites are filled with personal and demographic information. A Mashable article reported that SharesPost, a marketplace for shares in privately owned companies, suggested an $11.5 billion value for Facebook, a $1.4 billion value for Twitter and a $1.3 billion value for LinkedIn.[107] Forbes puts Facebook's market value higher than Lockheed Martin Corp., Boeing Co., Target, Inc., Sony Corp., Nike, Inc. and major automakers.[108] The driving force of Facebook's market value is access to all the information about the consumers that use the social network.[109] Douglas Rushkoff, an author and respected teacher of media studies at New York University and the New School

---

[101] *Id*.
[102] 18 U.S.C. § 1030 (2011).
[103] *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 519, *see also LaCourt v. Specific Media, Inc.*, No. SACV 10-1256-GW(JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011).
[104] *Id*. at 525
[105] *Id*.
[106] *Id*.
[107] Narasu Rebbapragada, *Facebook: How Much Is Your Personal Information Worth? **A**dvertisers And Hackers Could Make Mountains of Cash With The Data You Share On Social Networks*, PC WORLD, (June 21, 2010), http://features.techworld.com/sme/3227622/facebook-how-much-is-your-personal-information-worth/.
[108] Tom Foreman, *How Much Is Facebook Really Worth?*, CNNTECH, March 08, 2011, http://articles.cnn.com/201103-08/tech/facebook.overvalued_1_mark-zuckerberg-facebook-worldwide-users?_s=PM:TECH.
[109] *Id*.

University, said "We are the thing that Facebook has of value. We are the only thing they have to sell."[110] Lise Buyer of Class Five Group, a Silicon Valley firm that advises companies on going public, said, "Oh, Facebook is definitely worth something because it's a company that's collected more personal information about 600 million . . . individuals than any company has ever had access to before, and marketers love that information."[111]

Advocating for the worth of consumer's personal information, Ginsu Yoon co-founder of Cue Bynamite, a company with the purpose of helping consumers create some value for their online thumbprint, said, "There should be an economic opportunity on the consumer side."[112] He explains, "Nearly all the investment and technology is on the advertising side. Our view is that it's not about privacy protection but about giving users control over this valuable resource: their information."[113] For the courts to continuously hold that personal information has no economic value to its owner in the wake of the tremendous amounts of data and information that says otherwise, gives the power to the advertising companies to obtain valuable personal information from Internet users at no cost and through methods that violate global Internet standards.

In *Creative Computing*, the Ninth Circuit Court of Appeals held that loss of business and business goodwill constituted recoverable damages under the CFAA.[114] The court reasoned that "when an individual or firm's money or property are impaired in value, or money or property is lost, or money must be spent to restore or maintain some aspect of a business affected by a violation, those are economic damages."[115] The Ninth Circuit's reasoning can be applied to the loss of personal information as well. When personal information is stolen via the Internet, the victim must be proactive to ensure that their personal goodwill is not impaired in anyway. For example, if personal information that included credit card numbers, checking account numbers and passwords to protected accounts was stolen, the victim would need to take steps to prevent damage to their credit report. These proactive steps are costly to the victim. Unfortunately in many instances, damage to personal credit reports is nearly impossible to repair, and the damage can cost a person additional money in late fees and interest rates. Also, it is common knowledge that many businesses evaluate consumers credit reports before extending credit lines or offering in-store credit, a damaged, unfavorable credit report could cause a person's goodwill to diminish and seriously affect their ability to purchase necessary items. Thus, the *Creative Computing* court's holding should be applied to the loss of personal information and personal goodwill.

The courts repeatedly state in their orders dismissing these claims that plaintiffs alleging CFAA claims are unable to plead the threshold amount of damages required by the CFAA. In order for plaintiffs to plead the threshold amount of damages, the court must set a precedent detailing how to calculate the value of personal information. Furthermore, the courts must set a standard method of aggregation for damages under the CFAA because courts are split as to how damages should be aggregated under the statute.

Additionally, Congress recognizes the need for legislation to prevent and deter history sniffing and other online tracking practices.[116] Congress introduced at least nine bills since February 2011 that are designed to combat issues related to data collection and privacy on the web.[117] The House and Senate are making it a priority to provide the America people with legislation to guard against history sniffing and

---

[110] *Id*.
[111] *Id*.
[112] Sheila Shayon, *How Much Is Your Online Information Worth?*, (July 21, 2010), http://www.brandchannel.com/home/post/2010/07/21/Bynamite-Online-Security.aspx.
[113] *Id*.
[114] *Creative Computing*, 386 F.3d at 935.
[115] *Id*.
[116] Walter E. Judge & Matthew S. Borick, *History Sniffing: Updates On Current Litigation*, (Nov. 8, 2011), http://www.drm.com/news/2011/12/11/history-sniffing-updates-on-current-litigation/.
[117] *Id.* (The nine bills are as follows: H.R. 611 "Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (BEST PRACTICES) Act" (introduced Feb. 10, 2011); H.R. 654 "Do Not Track Me Online Act" (introduced on Feb. 11, 2011); S. 799 "Commercial Privacy Bill of Rights Act of 2011" (introduced April 12, 2011); H.R. 1528 "Consumer Privacy Protection Act of 2011" (introduced April 13, 2011); S. 913 "Do-Not-Track Online Act of 2011" (introduced on May 9, 2011); H.R. 1895 "Do Not Track Kids Act of 2011" (introduced May 13, 2011); S. 1151 "Personal Data Privacy and Security Act of 2011" (introduced June 7, 2011); S. 1408 "Data Breach Notification Act of 2011" (introduced July 22, 2011); and S. 1535 "Personal Data Protection and Breach Accountability Act of 2011" (introduced Sept. 8, 2011).

other online tracking practices.[118] Now, it is time for the courts to do their part in recognizing and combating the illegal wrongs individual Internet users are suffering at the hands of Internet advertising networks such as DoubleClick and Interclick.

5. Conclusion

Sonal Bose, along with countless other victims, have lost valuable personal information to Internet advertising companies through deceptive Internet practices, such as history sniffing and the placement of flash cookies. However, these individuals are unable to obtain their sought after relief under the CFAA because the federal courts refuse to find that personal and demographic information has significant value to its owner. The CFAA was enacted to protect against unauthorized access of computerized data. In order for the CFAA to serve that purpose, federal courts must make a determination as to the value of personal information, and decide on a standardized method for aggregating damages to reach the statutory threshold amount. If these issues are not addressed, victims of these illusive Internet procedures are left with no avenue to assert their rights.

* * * * *

Cite as: Arrington, Samantha .GOT COOKIES? Bose v. Interclick, Inc.: Computer Fraud and Abuse Act Claims Dismissed With Prejudice Due To Lack of Precedent Providing for the Value of Personal Information and an Unclear Standard for Aggregation of Damages. *Journal of International Commercial Law and Technology,* Vol.8 No.1 (January, 2013)

[118] *Id.*