Why do denial of service attacks reduce future visits? Switching costs vs. changing preferences

Avi Goldfarb*
Rotman School of Management
University of Toronto
105 St. George St.
Toronto, ON M5S 3E6
CANADA
(416) 946-8604
agoldfarb@rotman.utoronto.ca
http://www.rotman.utoronto.ca/~agoldfarb

February 2005

Abstract

This paper examines the denial of service attacks of February 2000 to determine the impact of an exogenous website shutdown on user behavior. The attacks had a lasting negative impact on six of the seven websites attacked (CNN, Yahoo, ZDNet, Amazon, Buy.com, and EBay, but not E*Trade). Using a new method to identify switching costs, the paper shows that, for Yahoo and the other free websites, this impact is due to switching costs benefiting the website visited instead of the attacked website. But for the online shopping websites, it is due to a lower opinion of the attacked website.

Keywords: denial of service attacks, Internet, switching costs, website shutdowns

* Thanks to Plurimus Corporation for providing me with the data, to Michael Whinston for an offhanded remark that lead to this paper, and to Ulrich Kaiser, and seminar participants at SUNY Buffalo, Rutgers University, and the BCRST conference for comments. This research was aided by a grant from the Social Science and Humanities Research Council of Canada's Initiative on the New Economy program.

1. Introduction

On February 7, 2000, a teenaged hacker nicknamed 'mafiaboy' shut down the Yahoo website for approximately three hours in the first of a wave of 'denial of service' (DoS) attacks.[1] Over the next two days, six other major websites would fall victim to mafiaboy's attacks, including Buy.com on the day of its initial public offering, Amazon, CNN, EBay, E*Trade, and ZDNet.

Website shutdowns are a frequent problem for Internet companies. In addition to numerous hacker attacks, websites often go offline due to technical problems. These problems could be the fault of the website itself or of some routing problem in the Internet architecture. In this paper, I show that the shutdowns due to the hacker attacks had an impact on user behavior. Users that could not access a website due to a DoS attack became less likely to visit that website in the future. By exploiting a 'natural experiment' in the data, I explore the cause of this impact. Broadly speaking, users may be less likely to return to the website for two reasons. First, the user's underlying opinion of the website may have changed. Since the user could not access the website, her view of the website's reliability and overall quality may be affected. On the other hand, the user may become locked-in to the website visited instead of the attacked website. Consequently, the user may not switch back to the attacked website once the attack is over.[2]

I can separate out these two effects due to a detailed data set that contains every website visited by 2651 households from December 27, 1999 to March 31, 2000. The DoS attacks therefore occurred roughly in the middle of the data set. The data set allows me to see whether users visited a competing website to the attacked website. For example, the data show whether a user visited MSN.com during the Yahoo attack. This fact allows identification of switching costs (lock-in) at the rival website separately from a change in preferences for Yahoo. Assuming users have no pre-existing systematic bias in the expected utility from the website visited during the attacks, if the impact is solely due to changing preferences, then all competing websites should gain a proportionally equal amount. If, on the other hand, there is a lock-in effect, then the website that is visited during the attack should gain more than other rival websites because the benefits of lock-in only accrue to that website. I discuss further identification issues in Section 4 and find evidence supporting the assumption of no systematic bias.

I find that DoS attacks do not have the same impact on all websites. While all attacked websites except E*Trade appear to have lost traffic due to the attacks, there is strong evidence only of switching costs benefiting competitors of Yahoo. There is weaker evidence that the lock-in effects matter for CNN and ZDNet. In general, my small sample of seven websites suggests that switching costs may be more likely to develop at competitors of free (to the user) websites as a consequence of DoS attacks than at competitors of shopping websites.[3] This suggests that online behavior needs to be understood in the context of the type of website visited.

---

[1] A DoS attack occurs when a hacker succeeds in shutting down a website. The most common type is a distributed DoS attack in which a hacker programs thousands of computers to request information simultaneously, thereby overloading the website's servers. Since the February 2000 attacks, DoS attacks have shut down dozens of websites, including most Microsoft websites in January 2001, Weather.com in May 2001, and Foxnews.com and ESPN.com in June 2002.

[2] This type of lock-in is often called true state dependence in the econometrics literature and short-run switching costs in the industrial organization literature. It is distinct from the longer-run switching costs faced by customers who want to change banks or move residences. While it is sometimes called "loyalty" (Keane 1997, Krishnamurthi and Raj 1991, etc.), it is different from the lay concept of loyalty. A truly "loyal" customer will not switch brands because a product is unavailable on one occasion.

[3] I use the terms 'online publisher' and 'free websites' interchangeably in this study. While not all free websites are publishers and not all publishers are free, the three free websites in the study (CNN, Yahoo, and ZDNet) are also the three publishers in the study. I cannot determine whether the consistent results across these websites in terms of state dependence occur because they are all publishers or because they are all free. By 'free', I mean that the main product available at the website has no extra monetary cost to the user. Therefore, Amazon is not

Understanding user behavior after a temporary website shutdown can help websites conduct damage control. First, knowing that users who try to access the website during the shutdown are less likely to return than they otherwise would be shows shutdowns do damage the websites and that at least some damage control is necessary. Second, if the impact is mainly a function of switching costs developed at the new website, then websites can perform short-run promotions to bring back old customers. Once the customer has returned, she will remain loyal. However, if the shutdown changes a user's perception of a website's reliability, then the website should focus promotional campaigns on the improved reliability of the website. In the case of a DoS attack, the website should emphasize that it has improved security against DoS attacks and that it is no more vulnerable than any other website to an attack. In other cases, it should argue that it has overcome the difficulties that led to the shutdown. In this way, it may be able to convince users that the bad experience at the website was a function of a one-time event that is unlikely to recur.

In his survey article on the economics of switching costs, Klemperer (1995, p. 515) emphasizes that "consumer switching costs give firms a degree of market power over their repeat-purchasers," implying that switching costs can lead to profits. This argument holds for the short-run switching costs identified in this paper as well as longer run switching costs of the kind that likely benefit E*Trade.

There remains, however, much disagreement as to whether there are switching costs of any kind in online business-to-consumer markets. On the one hand, Shapiro and Varian (1999) argue that the competition is just one click away and that consequently switching costs are negligible; Gandal (2001, p. 1105) claims that "there are little (if any) consumer switching costs" at Internet portals; and Porter (2001, p. 69) argues the online "cost of switching is low." Alternatively, there is a considerable literature in marketing showing that consumers exhibit lock-in to particular brands, even when switching costs should be zero. Danaher, Wilson, and Davis (2003) and Zauberman (2003) both find that repeat purchase behavior is high online. In an online context, Johnson, Bellman, and Lohse (2003) label the cost of thinking involved in switching websites "cognitive switching costs."

This debate is part of the larger discussion about frictionless markets on the Internet. Starting with Bakos (1997), there has been an ongoing debate about whether online markets are frictionless. Brynjolfsson and Smith (2000), Clay, Krishnan, and Wolff (2001), Pan, Ratchford, and Shankar (2002), and many others find that there is online price dispersion in e-tail markets, suggesting these markets are not frictionless. Hann and Terwiesch (2003) find small, but statistically significant, frictions in online shopping. The present study measures frictions in e-tail and online publishing markets.

I find evidence that grouping all online markets together is misleading. Lock-in develops differently for users at different websites. In general, for shopping websites, Shapiro and Varian's argument appears to hold. When spending money, it seems that trust and reliability are more important than the website visited most recently. For Yahoo and perhaps some other free websites, being at the top of a user's mind may be sufficient to bring a user to that website. The switching costs, however small, matter.

A number of different methods to identify switching costs exist in consumer markets. Typically, switching costs are identified by an individual's propensity to return to a website beyond the average propensity of that individual to visit the website. This method is used by Jones and Landwehr (1988), Keane (1997), Seetharaman, Ainslie, and Chintagunta (1999), and many others. It relies on assumptions about the influence of individual heterogeneity on serial correlation in the error term. Chen and Hitt (2002) exploit differences in the behavior of old and new customers of Internet brokerage firms to see whether the old customers are loyal. They rely on the assumption that all customers have the same overall preferences. I present a new way to identify switching costs that relies on an assumption about the substitutability of different websites.

This method could be applied to measuring switching costs when a product is unavailable in a grocery store for an exogenous reason. These 'stockouts' have been explored in other contexts by

---

considered free, even though it is free to access the website. The main products available at Amazon (books, CDs, etc.) have a monetary cost.

Jeuland (1979), Farquhar and Pratkanis (1993), Balachander and Farquhar (1994), and others. To my knowledge, they have not been used to measure the importance of switching costs in a product category.

The next section will give a brief description of the data set. Using a difference-in-difference econometric methodology, section 3 shows that the DoS attacks negatively impacted six of the seven attacked websites. Section 4 then shows that lock-in to the website visited during the attack played an important role for Yahoo and perhaps the other free websites and little role for the shopping websites. Section 5 concludes that short-run promotional campaigns may overcome much of the negative impact of a website shutdown for free websites, but shopping websites will have to develop more comprehensive strategies aimed at winning back customers' confidence.

2. Data

The raw data set, courtesy of Plurimus Corporation, consists of every website visited by 2,651 households between December 27, 1999 and March 31, 2000 for a total of 3,228,595 observations. On average, therefore, there are 1,217 observations per household. In addition, the data set contains the time of arrival at and departure from a website (to the second), the number of pages viewed at a website, the number of bytes downloaded from the website, and the number of bytes uploaded to the website.

The data set has a number of limitations. First, it is collected at the household level rather than at the individual level. One individual could be online during the DoS attack and never again be online during the sample. All other observations could be another individual. If this is the case, being online for the DoS attack will have no effect. Second, there is no at-work data. It is possible that members of the control group attempted to access a website from work during a DoS attack. Both of these limitations, however, will bias the results toward finding no effect for the attacks and I find an effect. Also the data is not geographically representative, and it does not include AOL users. These are unlikely to have an impact on the results in this study.

The websites are divided into categories. In each category are all major competitors of the attacked website. For example, competitors to Yahoo include MSN.com, Altavista, Lycos, Google, and dozens of other search engines and portals. Plurimus Corporation initially set the category definitions.

I join this data set with a data set of 'media mentions' constructed from the Lexis-Nexis Academic Universe database. If one of the seven companies hit with a DoS attack is mentioned at least once on any of the network television news broadcasts (ABC, CBS, or NBC), or in the New York Times, then the media mentions variable is equal to one for that day. Also, if a company is mentioned at least once in the Pittsburgh Post-Gazette, the Tampa Tribune, the Dallas Observer, the Greensboro News and Record, or the Durham Herald-Sun, then media mentions is equal to one for local residents on that day.

The other essential piece of data for this study is the identification of the timing of the DoS attacks. CNET Online (Sandoval and Wolverton 2000) printed the exact times that each attack started and finished, shown in Table 1. Table 1 also shows the number of households in the sample online at the time of the attacks as well as the number of households that visited a website in the category of the attacked website during the attack.

Following the language used, for example, in Manski (1995), those households that experienced the DoS attacks are called the 'treatment group' while those that did not are called the 'control group.' The treatment group received the stimulus of the DoS attack. The control group did not.

Since the websites were inaccessible, I cannot determine whether a household tried to access the website under attack and therefore cannot perfectly identify the treatment and control groups. Consequently, I estimate a probability for each household that is in the treatment group of having experienced the DoS attack. First, if the household was not online during the attack, then it is assigned zero probability of having experienced the attack. Second, household fixed effect probit regressions were run on the pre-attack sample to predict the probability that a given visit during the attack was to

the attacked website. The regressions are based only on the attacked website and its competitors, and the covariates are the previous website chosen, media mentions, the log of bytes uploaded to the attacked website on the previous visit, and the log of bytes uploaded to any competing website on the previous visit. If a household visited more than one website during the attack then the probability of being in the treatment group is the probability that the first visit was to the attacked website plus the probability that the second was to the attacked given that the first was not plus the probability that the third was to the attacked given that the first and second were not and so on.

While this definition gives a good sense of whether someone in the household tried to visit the attacked website during the attack, determining the reasons behind the effect (section 4 below) involves understanding whether the visit to a website that was not attacked was out of character. For this reason, I also present results for a different measure of whether the household is in the treatment group. In this measure, I take the pre-attack propensity of the household to visit the website actually visited during the attack and subtract it from one. In particular, if all visits in that category before the attack are to that website, then this has a value of zero; if the household has never visited the website before, then this has a value of one; and there is a continuum of values in between. Rather than identifying how likely it was that the household has experienced the attack, this measures whether the website visited instead was out of character.[4]

3. The Total Effect of the Denial of Service Attacks

3.1 Models and Identification

I determine the total effect of DoS attacks on the websites hit by the attacks using a discrete choice utility maximization framework. I believe this framework is best because it is built from an explicit economic model of utility and because it allows for the effects of the attack to decrease over time.[5] As I will argue below, this time dimension provides a further method for separately identifying switching costs from changing preferences. I also show that the results are robust to a probabilistic differences framework as recommended in Bertrand, Duflo, and Mullainathan (2004) and a duration model framework.

In all models, I look at the impact on users who have experienced the attack relative to their previous behavior and to changes in the behavior of others. This methodology can therefore be seen as a difference-in-difference approach. I look at the behavior of the treatment group (the group that experienced the DoS attacks) after the attacks occurred. I compare this behavior with that group's behavior before the attacks—the first difference—and with the other group's behavior after the attacks—the second difference. In this way, the econometric method borrows from Milyo and Waldfogel's (1999) study of the effects of advertising on prices, from Manski's (1995) discussion of identification in econometric models, and from other studies of treatment effects.

3.1.1 Utility Maximization Discrete Choice Models

For the utility maximization models, I assume that Internet users choose the website that they expect will give them the highest utility on any particular choice occasion. For the shopping websites (Amazon, Buy.com, and EBay), this means that they go to the website that is most likely to have a product they want at an affordable price. For information services (CNN, ZDNet), this means users go to the website they expect will provide them with interesting information in an efficient manner. For

[4] I also use one more measure of the probability of being in the treatment group to check the robustness of the above definitions. Instead of using the regression predictions, I estimate the probability that a given household goes to the attacked website during the attack as its prior propensity to visit the website. Unlike the regressions, this estimate is based on all website visits by the household, rather than just category visits. For example, 41% of household 237's website visits prior to the attack are to Yahoo. This household visited two websites during the attack. Therefore the estimated probability of being in the treatment group is 0.41+(1-0.41)0.41=0.65.

[5] Telang, Boatwright, and Mukhopadhyay (2004) show the importance of controlling for time between visits in website choice models.

search engines (Yahoo), they choose the website that will give them a high probability of finding what they seek in a small amount of time. For financial services (E*Trade), they choose the website that will allow them to conduct financial transactions efficiently and securely given their previous relationships.

The expected utility from visiting a website is then a function of past experience at the website, website characteristics, and an idiosyncratic error term. Formally, household i chooses website j on choice occasion t when

$$Eu_{ijt} \geq Eu_{ikt} \quad (1)$$

for all $k \neq j$. Where Eu_{ijt} is the expected utility and is defined by

$$Eu_{ijt} = T_{ij}\gamma + A_{jt}\theta + \boldsymbol{T_{ij}A_{jt}\alpha} + D_{jt}\delta + \boldsymbol{D_{jt}T_{ij}\lambda} + X_{ijt}\beta + \mu_{ij} + \varepsilon_{ijt} \quad (2)$$

Here T_{ij} is the probability of being in the treatment group, A_{jt} is equal to one if the attacks have already happened and zero otherwise, D_{jt} is the number of days since the attack occurred (it is equal to zero before the attack), X_{ijt} are the other covariates included in the model, μ_{ij} is the household-level brand preference, and ε_{ijt} is the idiosyncratic error term. The treatment effect is therefore identified by the coefficient α, or the interaction between being in the treatment group and whether the attacks have occurred. The coefficient λ measures the decay of this effect over time. The other covariates function as controls that allow for identification of the (treatment) effect of the website shutdown caused by the DoS attacks. Since the data set is only three months long, long-run switching costs are subsumed into the household-level effect μ_{ia}.

The results presented are probit models where the dependent variable is a dummy variable for whether the individual visits the website hit with the DoS attack (CNN, Yahoo, etc) on a particular visit.[6] For example, when estimating the impact of a DoS attack on Amazon users, $y_{it}=1$ when a household visits Amazon, and $y_{it}=0$ otherwise. The baseline model is a random effects model where μ_{ij} is distributed i.i.d. Normal, and X_{ijt} includes whether the individual chose the attacked website on the previous choice occasion, whether the attacked website was mentioned in the media that day, and the previous experience at the attacked website and a competing website in terms of the log of bytes uploaded to the website on the previous visit.[7] Media mentions and previous experience are included as other factors that may affect choice. The website visited on the previous choice occasion is included to avoid mixing the overall loyalty effect with the direct effect of the DoS attack. Without this variable, the measured effect of the attacks increases. The econometric analysis identifies whether a household who experienced the attack changes its behavior relative to one that did not experience the attack.

3.1.2 Robustness Checks: Probabilistic Differences and Duration Models

In order to ensure the results are not merely a function of the model chosen, I conduct two robustness checks: probabilistic differences and duration models. The probabilistic differences specification splits the panel into two parts: everything that happened before the DoS attack and everything that happened after it. This method is recommended by Bertrand, Duflo, and Mullainathan

[6] I use probit models rather than multinomial logit models because the probits do not obscure the main identification arguments decribed above and in section 4.1. In this context, I believe the the clarity of the probit identification dominates any extra information that a multinomial logit may allow. Nevertheless, preliminary regressions in the multinomial logit format suggest that the main qualitative results do not change

[7] Bytes downloaded from the website, pages viewed, and time spent had the same general effect as bytes uploaded to the website with less explanatory power. Due to the skewness of this variable, the logarithm of bytes uploaded was used.

(2004) for identifying difference-in-difference effects when there is serial correlation in outcomes and the number of individuals is small.[8]

For each household in the data set, I calculate the household-level market share of the attacked website relative to its competition in the month and a half before and the month and a half after the DoS attacks. The model now consists of the following two equations:

$$P_{i1} = X_{i1}\beta + Z_i\gamma + \mu_i + \varepsilon_{i1} \quad (3)$$

$$P_{i2} = Pr_i\alpha + X_{i2}\beta + Z_i\gamma + \mu_i + \varepsilon_{i2} \quad (4)$$

Here, P_{i1} is the household-level market share for the attacked website before it is attacked, and P_{i2} is the household-level market share for the attacked website after it is attacked. The probability of experiencing the DoS attack is Pr_i. The time-varying covariates are X_{it}, the time-invariant covariates are Z_i, the household-specific fixed effect is μ_i, and the idiosyncratic error term is ε_{it}. The coefficients for Pr_i, X_{it}, and Z_i are α, β, and γ respectively.

Differencing these two equations gives the model I estimate:

$$P_{i2} - P_{i1} = Pr_i\alpha + (X_{i2} - X_{i1})\beta + \varepsilon_{i2} - \varepsilon_{i1} \quad (5)$$

The fixed effects and time invariant effects cancel out, and the remaining model that can be consistently estimated by OLS.[9] For most estimates, I assume there are no time-varying covariates. The effect of the DoS attack is measured by the coefficient on the Pr_i variable, α. This probabilistic differences model can be viewed as an examination of correlations between the probability of being in the treatment group and the change in visit propensity without forcing a parametric form on any household-level characteristics or on serial correlation in the error terms. One weakness of this model relative to the utility maximization model, however, is it does not allow for decay in the impact of the attacks over time. Another is that it is not based on an economic model of decision-making.[10]

I also present results for an exponential duration model (Lancaster 1990). In this model, I estimate whether the time until the first visit to the attacked website following the attack takes longer than expected. In particular, the dependent variable becomes days between visits to the website (where visits on the same day are counted as one day). The model includes controls for being in the treatment group, being the first visit after the attacks, and recent experience at the website in terms of bytes uploaded on the previous visit. The variable of interest is the interaction effect of being in the treatment group and being the first visit after the attacks.

I choose an exponential model because the covariates are easy to interpret due to the constant hazard rate. It is not the hazard rate itself that is of interest, but the shifts in the hazard rate due to changes in the covariates. The main qualitative results of the duration model are identical if a weibull, lognormal, cox proportional hazard, or poisson count model is used instead of an exponential model.

Telang, Boatwright, and Mukhopadhyay (2004) use a more sophisticated duration model and similar data to estimate intervisit time to search engines. Their model controls for the periodicity of

---

[8] They argue that standard errors are inconsistent in this case unless there are a large number of individuals and some sort of individual-level effect is included. This suggests that this method will be particularly effective for understanding the impact of the DoS attacks on Amazon, EBay, E*Trade, and ZDNet.

[9] Greene (1997, pp. 277) explains that normality of the estimator does not depend on normality on the disturbance as the number of observations grows. Consequently, the coefficients and standard errors can be estimated with standard OLS techniques.

[10] The Berry (1994) structured framework may seem like an appealing model for probabilistic differences because it is based on a utility maximization framework; however, it has two weaknesses in this context. First, the fixed effects do not get differenced out and consequently need to be estimated for each household. Second, there are many households with zero visits in either the before or after period. This leads to difficulty because this model requires the log of market share.

Internet visit data and is effective at predicting time between category visits. They, however, are interested in category rather than brand specific visits (p. 210), and their method therefore does not allow for brand choice. The reason I place little emphasis on the duration model is that without brand choice, the duration model does not allow identification of switching costs. This means that there is no switching in the model. The duration model results, however, do show that the attacks did have a short-run negative impact on the attacked websites.

3. 2 Results: The Total Effect of the Denial of Service Attacks

Tables 2 through 4 show the impact of mafiaboy's DoS attacks. Table 2 presents random effects probit regressions using the baseline regression described in section 3.1.1 for each of the seven attacked websites. The top part of the table presents coefficients and the bottom part presents marginal effects. The first row shows that the DoS attacks had a negative impact on the probability of visiting each attacked website except E*Trade. The marginal effects range from 0.8% for Buy.com to nearly 8% for ZDNet. These marginal effects measure the decrease in the probability of visiting the website for the average household in the treatment group after the attack. For example, the marginal effect of –3.9% for Yahoo means that households that experienced the attack visit Yahoo 3.9% less than before, relative to other households that did not experience the attack.

The second row shows that the effect of the attack decays for the free websites (CNN, Yahoo, and ZDNet), but not for the other websites. In other words, the attacks had a negative impact on all free and shopping websites. This effect decreased over time for the free websites but not for the shopping websites.

Since the number of households that likely experienced the attack is much larger for the Yahoo attack than for the others and since the number of choice occasions in Yahoo's portal category is much higher than for the others, I present many robustness results for Yahoo that I do not present for the other categories.[11] Throughout the paper, I emphasize the strength of the Yahoo results relative to the others. Table 3 presents these other specifications and shows that the general results change little with specification. Column 2 shows that the results hold in a fixed effects framework. Column 3 shows that the effect holds without the decay function. Column 4 shows, as expected, that the results are even stronger when the variable on website chosen on the last choice occasion is not included. Columns 5 and 6 show that the results hold with different definitions of the treatment group.

Table 4 presents the coefficients on the treatment effect for the probabilistic differences and duration models. The results do not generally change, although some of the coefficients are no longer significantly different from zero with 90% confidence. The general trend of the table, however, is the same: the denial of service attacks had a negative effect of visits to CNN, ZDNet, Amazon, Buy.com, EBay, and especially Yahoo. They do not appear to have had a negative effect on E*Trade. Since E*Trade users tend to have accounts and a strong relationship with the company, it is not surprising that a short DoS attack was insufficient to cause users to abandon their discount broker. This distinction between short-term and long-term switching costs is essential to identifying short-term switching costs in the next section.

4. Switching Costs or Changing Preferences?

4.1 Models and Identification

In order to identify whether the competing websites visited during the attack benefited from switching costs, I use the fact that switching costs resulting from the attacks will only affect websites that the users visit during the attack. All other websites competing with the attacked website can only benefit from a change in preferences or a loss of switching costs to the attacked website.

[11] Presenting these results for all seven websites is beyond the space limitations of Management Science. In general, the qualitative results are the same except that significance often goes away. Furthermore, the fixed effects results are not reliable as there are often fewer than 10 observations per household in the other categories.

The switching costs identified are then those that accrue at the website visited instead of the attacked website during the attack. For example, suppose household *i* visits MSN.com instead of Yahoo during the attack on Yahoo. MSN benefits from a switching cost if it gains more than Altavista and Lycos as a consequence of the attack. Otherwise, the gain to MSN is just a consequence of the loss to Yahoo.

This assumes that households, on average, have accurate information about the quality of websites. For example, instead of a switching cost, it could be that consumers systematically underestimate the utility from the website visited instead of the attacked website. Upon visiting the website, their image of the site improves, and they become more likely to visit in the future. I will examine this assumption by looking at whether the effect decays over time. If the effect decays over time, this means there is reversion to the state that occurred before the attacks. This would suggest that the users' preferences before the attacks were on average correct, providing support for the assumption and the identification argument.

4.1.1 Utility Maximization Discrete Choice Models

In the utility maximization framework, recall equation (2):

$$Eu_{ijt} = T_{ij}\gamma + A_{jt}\theta + \boldsymbol{T_{ij}A_{jt}\alpha} + D_{jt}\delta + \boldsymbol{D_{jt}T_{ij}\lambda} + X_{ijt}\beta + \mu_{ij} + \varepsilon_{ijt}$$

The key to the identification of switching costs at the websites visited during the attacks is that $T_{ij}A_{jt}\alpha$ will have a different meaning for competing websites that were visited during the attack and those that were not. The utility of returning to a website that was visited during the attack will have a lock-in (or short-run switching cost) component. Other competing websites to the attacked website will not benefit from lock-in. They will only benefit from the reduced propensity to visit the attacked website. Therefore, the utility from visiting the attacked website for a household that experienced the attack is

$$Eu_{iat} = T_{ia}\gamma_{\boldsymbol{a}} + A_{at}\theta_{\boldsymbol{a}} + \boldsymbol{T_{ia}A_{at}\alpha_a} + D_{at}\delta_{\boldsymbol{a}} + D_{at}T_{ia}\lambda_{\boldsymbol{a}} + X_{iat}\beta + \mu_{ia} + \varepsilon_{iat} \quad (6)$$

Here α_a is the preference change as a consequence of the attack combined with any decrease in switching costs associated with the attacked website. As mentioned before, long-run switching costs are subsumed into the household-level effect μ_{ia}. The utility from visiting a competing website that was visited during the attack is

$$Eu_{ict} = T_{ic}\gamma_c + A_{ct}\theta_c + \boldsymbol{T_{ic}A_{ct}\alpha_c} + D_{ct}\delta_c + D_{ct}T_{ic}\lambda_c + X_{ict}\beta + \mu_{ic} + \varepsilon_{ict} \quad (7)$$

Here α_c is the added lock-in associated with having visited the website an extra time in the past due to the DoS attack. Finally, the utility from visiting another competing website that was not visited during the attack is

$$Eu_{iot} = X_{iot}\beta + \mu_{io} + \varepsilon_{iot} \quad (8)$$

The DoS attack will not directly enter the utility function for a website that was neither attacked nor visited during the attack. The attack will only affect the probability of visiting these other websites through the impact on the attacked websites and the websites that were visited during the attack. Controlling for user behavior before the attacks, $\boldsymbol{\alpha_c}$, the coefficient on lock-in is therefore identified by exploring whether users are more likely to visit websites that they visited during the attack than other competing websites.

In particular, a household visits the website that was visited during the attack instead of another competing website if $Eu_{ict} \geq Eu_{iot}$. Rearranging terms, this means that the website visited during the attack is visited again if

(9) $$T_{ic}\gamma_c+A_{ct}\theta_c+\boldsymbol{T_{ic}A_{ct}\alpha_c}+D_{ct}\delta_c+\boldsymbol{D_{ct}T_{ic}\lambda_c}+(X_{ict}-X_{iot})\beta+\mu_{ic}-\mu_{io}+\varepsilon_{ict}-\varepsilon_{iot}\geq 0$$

Therefore, estimating a choice model to see whether competing firms that were visited during the attacks gained more than other competing firms will identify the effect of lock-in, $\boldsymbol{\alpha_c}$. In addition to covariates used in section 3, a proxy for substitutability is also used. [12]

This will allow for identification of short-run switching costs accruing to the website visited during the DoS attack. This method does not identify whether there are switching costs at the attacked websites. In the case of E*Trade, there are likely strong long-run switching costs that meant the attacks had no effect. As mentioned earlier, the method relies on the assumption that households on average do not underestimate their expected utility to visiting the website visited during the DoS attack before the attack. If λ is negative, however, then behavior reverts to that which occurred before the attacks. Reversion would suggest that expected utility from the attacked website was not systematically underestimated.

4.1.2 Robustness Checks: Probabilistic Differences and Duration Models

Under the probabilistic differences specification, before the attack, the probability of visiting the competing website that was used during the attack will be

(10) $$P_{ic1}= \overline{X}_{ic1}\overline{\beta}+Z_{ic}\gamma+\mu_{ic}+\varepsilon_{ic1}$$

After the attack, the probability will be

(11) $$P_{ic2}= Pr_i\alpha+ \overline{X}_{ic2}\overline{\beta}+Z_{ic}\gamma+\mu_{ic}+\varepsilon_{ic2}$$

where α is the added lock-in associated with having visited the website an extra time in the past due to the DoS attack. Since the identification relies on the difference between the website visited during the attack relative to other competing websites and not on the attacked website itself, the probabilities are estimated excluding the attacked website. Formally, let $Nvisits_{ict}$ be the number of visits to the website visited during the attack in period t, and let $Nvisits_{iot}$ be the number of visits to all other websites besides the attacked website. Then,

(12) $$P_{ict}=Nvisits_{ict}/(Nvisits_{ict}+Nvisits_{iot})$$

Therefore, the probabilistic difference model will give

(13) $$P_{ic2}-P_{ic1} = Pr_i\alpha + (\overline{X}_{ic2} - \overline{X}_{ic1})\overline{\beta} + (\varepsilon_{ic2}-\varepsilon_{ic1})$$

As in section 3, this can be consistently estimated by OLS. As mentioned earlier, the identification relies on the no systematic bias in the expected utility from the websites visited during the attacks. Unlike the utility maximization models presented in section 4.1.1, the probabilistic differences method cannot provide evidence in favor of retaining this assumption.

Duration models cannot identify switching costs since only one website is used in the measurement. They cannot separate a change in preferences for the attacked website from a switching

[12] This variable is defined as the $(PG_c-PG_a)^2-(PG_o-PG_a)^2$ where PG_j is average number of pages viewed at website j, c is the competing website visited during the attack, a is the attacked website, and o is other competing websites that were not visited during the attack. Pages are used rather than time spent because it has more explanatory power in terms of the log likelihood. The reasons for including this variable are discussed in section 4.1.3.

cost accruing to the website visited during the attack. Nevertheless, I show the results of an exponential duration model in order to show whether the websites visited during the attack were visited disproportionately soon after the attack. As in section 3, the main qualitative results of the duration model are identical if a weibull, lognormal, cox proportional hazard, or poisson count model is used instead of an exponential model.

4.1.3 Model Discussion

This identification, however, is imperfect. Another possibility for the competing firm that was visited during the attack gaining more than other competing firms may be that the competing firm is a closer substitute for the attacked firm. Consequently, when households leave the attacked firm for preference reasons, they will go to the firm visited during the attack. The probabilistic differences model largely overcomes this potential issue by differencing out all household-level preferences that are time-invariant. Similarly, the household-level effects in the discrete choice models help control for this issue. I also include measures of substitutability based on user behavior at the websites. Furthermore, there is little reason to believe this would only be relevant at free websites and not at shopping websites. These controls do not perfectly overcome the obstacle to identification cited above; however, the method relies on a different, and perhaps weaker, set of assumptions than other methods used to identify lock-in.

As discussed earlier, the model assumes no systematic bias in preferences for the website visited during the attack. While a decay in the effect of the attacks would suggest that there is no systematic bias, it cannot be completely ruled out as an explanation.

It is important to remember that this method identifies a particular kind of lock-in: the impact of an exogenous one-time switch on the website that benefited from the switch. All that is required for the lock-in effect to exist is that the act of visiting a website once will increase the probability of visiting that website in the future, all else being equal including preferences for that website not based on this lock-in effect. Having visited a website at some point in the past must therefore have a lasting impact on the utility from visiting that website in the future.[13] Nevertheless, such a finding of state dependence does not preclude a change in preferences as well. The relative importance of lock-in and changing preferences for the Yahoo attack are discussed briefly at the end of section 4.2.

4.2 Results: Switching Costs

Tables 5 though 8 show the estimates of whether short-run switching costs accrued to the websites visited during the DoS attacks. Table 5 shows the utility maximization baseline model results for all the attacks using the same treatment group definition as in section 3: the probability that the household tried to access the attacked website but could not based on the past propensity to visit the site. In Table 6, the treatment group is defined by the degree to which the visit that occurred during the DoS attack was out of character for the household. This table shows whether the measure of switching costs accrued especially to households that visited websites that they do not normally visit. Table 7 shows more results for the attack on Yahoo, and Table 8 presents probabilistic differences and duration model results.

The most striking result relates to the Yahoo attack. In all models in all tables, the coefficient on the interaction of being in the treatment group and being after the attack occurred is positive and strongly significant. Furthermore, this effect decays over time. In other words, there is strong evidence that switching costs accrued to the websites visited instead of Yahoo during the attack on Yahoo.

The results for the websites visited during the CNN and ZDNet attacks are always positive, again suggesting switching costs. However, the results for CNN are only significant in the utility maximization discrete choice models, and the results for ZDNet are only significant in the probabilistic differences models. None of the other websites have consistently positive results. For these reasons, I conclude that switching costs accrued to websites visited during the attack on Yahoo; they also

[13] An example of this framework is Guadagni and Little's (1983) loyalty measure.

probably accrued to those visited during the attacks on CNN and ZDNet; it is unlikely they accrued to those visited during the attacks on Amazon, Buy.com, EBay, and E*Trade. In other words, they seem to have accrued to free websites but not shopping websites.

As described earlier, the identification of switching costs assumes that there is no systematic bias in estimates of expected utility from the website visited during the attack before the attack occurred. I argued that if the effect of the attacks decays over time, then this assumption is likely valid. The results on CNN and Yahoo in Tables 5, 6, and 7 all show that the effect of the attacks decays over time. Since there are no significant results for ZDNet in these tables, I cannot reject the possibility of systematic bias for ZDNet. Therefore, I conclude that it is unlikely that the effects for Yahoo and CNN are a result of a change in preferences due to the attacks. They are more likely a result of a short-run switching cost benefiting the website visited during the attack.

Column 4 of Table 7 shows a model where the dependent variable is equal to one if the website visited during the attack is visited and zero if either the attacked website or another website in the category is visited. This identifies the total effect of the attacks, including both the effects on preferences (or perhaps switching costs) at the attacked website as well as the switching cost effect at the website visited during the attack. Comparing this column to the baseline model shows that 56.7% of the total effect of the attacks on Yahoo is due to the effect on the rival rather than Yahoo. The decay results suggest this is likely a switching cost. For CNN, the results are different. 98.6% of the effect appears to be due to switching costs accruing to the website visited during the attack.[14] I do not present the results for ZDNet, the shopping websites, and E*Trade because the coefficients identifying switching costs are not significantly positive in the utility maximization model. Nevertheless, for both Yahoo and CNN, over half of the drop in the market share of the attacked website is due to switching costs accruing to the website visited during the attack.

5. Conclusions

The denial of service attacks of February 2000 provide a natural experiment for exploring the impact of an exogenous website shutdown on user behavior. Unless there are large long-run costs of switching websites, as in the case of E*Trade, users are less likely to return to websites if they cannot access them, even if only for a short period of time.

For Yahoo, this impact is partly a result of users developing switching costs to its competitors as a consequence of visiting a rival website during the attack. For CNN and ZDNet, it likely also is partly a result of switching costs accruing to users at their competitors. It is not only a function of a change in the user's underlying opinion of the attacked website nor a loss in switching costs to the attacked website. Switching costs, however, do not seem to have played a major role in the impact of the DoS attacks on shopping websites.

Even though the competition to the free websites is just a click away, the potential benefits to switching seem to be dominated by the switching costs generated by one forced visit to a free website. Despite no obvious impediments to switching websites and controlling for overall preferences, one visit generates a lasting effect.

For shopping websites, this is not the case. Perhaps the potentially larger perceived benefits surrounding the pricing and quality of a user's favorite shopping website mean that the lock-in benefits associated with a one-time switch are not large enough to be relevant to online shoppers.

Each of these DoS attacks lasted less than four hours. Therefore, I can only identify the impact of a brief one-time switch. It is likely that the results would be different if the attacks lasted for days. In this case, it is likely that some E*Trade customers may switch, and identifying different types of switching costs would be possible. I do not presume to identify the impact of a long-term shutdown of a website.

[14] These results are not presented in a table. The marginal treatment effect of this regression is 0.204.

The identification method used here to estimate switching costs could easily be applied to stockouts in grocery stores. Comparing the impact of the stockout on the brand that is bought instead with other brands that are not bought will allow identification of switching costs in these markets.

The reasons behind the impact of a DoS attack, or any short-term shutdown, on a website have important strategic implications for websites. In general, the results suggest that online behavior needs to be understood in the context of the type of website visited. The above analysis suggests that free websites will benefit from a short promotional campaign aimed at those users who try to access the website during the shutdown. The lock-in effects will then accrue to the promoting website again, and the impact of the shutdown will be minimized.

Shopping websites, on the other hand, are less likely to find this a useful strategy. They should focus on showing customers that the concerns that arose from the shutdown are no longer valid. Shopping websites that are victims of DoS attacks should emphasize to the customers that try to access the website during that attack that they have improved security and are no more vulnerable than any other websites to an attack. Shopping websites that shut down for technical reasons should emphasize that the problem is unlikely to recur.

References

Balachander, Subramanian and Peter H. Farquhar. 1994. "Gaining More by Stocking Less: A Competitive Analysis of Product Availability." *Marketing Science* 13(1), 3-22

Bakos, J. Yannis. 1997. "Reducing Buyer Search Costs: Implications for Electronic Marketplaces". *Management Science*. 43 (12 Dec.). 1676-1692.

Berry, Steven T. 1994. "Estimating Discrete-Choice Models of Product Differentiation." *RAND Journal of Economics* 25: 242-262.

Bertrand, Marianne, Esther Duflo, Sendhil Mullainathan. 2004. "How Much Should We Trust Differences-in-Differences Estimates?" *Quarterly Journal of Economics* 119(1), 249-275.

Brynjolfsson, Erik, and Smith, Michael D. 2000. "Frictionless Commerce? A Comparison of Internet and Conventional Retailers." *Management Science* 46(4 April), 563-585.

Chen, Pei-Yu and Lorin M. Hitt. 2002. "Measuring Switching Costs and the Determinants of Customer Retention in Internet-Enabled Businesses: A Study of the Online Brokerage Industry." *Information Systems Research* 13 (3 Sept.),. 255-274.

Clay, Karen, Krishnan, Ramayya, and Wolff, Eric. 2001. "Prices and Price Dispersion on the Web: Evidence from the Online Book Industry." *Journal of Industrial Economics* 49(4), 521-540.

Danaher, Peter J., Isaac W. Wilson, and Robert A. Davis. 2003. "A Comparison of Online and Offline Consumer Brand Loyalty." *Marketing Science* 22(4 Fall), 461-476.

Farquhar, Peter H., and Anthony R. Pratkanis. 1993. "Decision Structuring with Phantom Alternatives." *Management Science* 39(10), 1214-1226.

Gandal, Neil. 2001. "The Dynamics of Competition in the Internet Search Engine Market." *International Journal of Industrial Organization* 19: 1103-1117.

Greene, William H. 1997. *Econometric Analysis*. 3rd Ed. Upper Saddle River, NJ: Prentice Hall.

Hann, Il-Horn, and Christian Terwiesch. 2003. "Measuring the Frictional Costs of Online Transactions: The Case of a Name-Your-Own-Price Channel." *Management Science* 49(11 Nov.), 1563-1579.

Heckman, James J. 1981. "Statistical Models for Discrete Panel Data." In *Structural Analysis of Discrete Data with Econometric Applications.* Ed. Charles F. Manski and Daniel McFadden, 179-195. Cambridge, MA: The MIT Press.

Jeuland, Abel P. 1979. "The Interaction Effect of Preference and Availability on Brand Switching and Market Share." *Management Science* 25(10), 953-965.

Johnson, Eric J., Bellman, Steven, and Lohse, Gerald L. 2003. "Cognitive Lock-In and the Power Law of Practice." *Journal of Marketing* 57(2 April), pp. 62-75.

Jones, J. Morgan, and Jane T. Landwehr. 1988. "Removing Heterogeneity Bias from Logit Models Estimation." *Marketing Science* 7(1), 41-59.

Keane, Michael P. 1997. "Modeling Heterogeneity and State Dependence in Consumer Choice Behavior." *Journal of Business and Economic Statistics* 15(3), 310-327.
Klemperer, Paul. 1995. "Competition when Consumers have Switching Costs." *Review of Economic Studies* 62: 515-539.
Lancaster, Tony. 1990. *The Econometric Analysis of Transition Data.* Cambridge University Press: Cambridge UK.
Manski, Charles. 1995. *Identification Problems in the Social Sciences.* Cambridge, MA: Harvard University Press.
Milyo, Jeffrey and Joel Waldfogel. 1999. "The Effect of Advertising on Prices: Evidence in the Wake of 44 Liquormart." *American Economic Review* 89(5), 1081-1096.
Pan, Xing, Ratchford, Brian, and Shankar, Vankatesh. 2002. "Can Price Dispersion in Online Markets be Explained by Differences in E-tailer Service Quality?" *Journal of the Academy of Marketing Science* 30(4), pp. 429-441.
Porter, Michael E. 2001. "Strategy and the Internet." *Harvard Business Review*. 79(3 March), 62-78.
Sandoval, Greg, and Troy Wolverton. 2000. "Leading Web Sites under Attack." *CNET News.com*. February 9, posted 1:50PM PT. http://news.com.com/2100-1017-236683.html.
Seetharaman, P. B., Andrew Ainslie, and Pradeep Chintagunta. 1999. "Investigating Household State Dependence Effects Across Categories." *Journal of Marketing Research* 36(4), 488-500.
Shapiro, Carl, and Hal R. Varian. 1999. *Information Rules: A Strategic Guide to the Network Economy*. Boston: Harvard Business School Press.
Telang, Rahul, Peter Boatwright, and Tridas Mukhopadhyay. 2004. A Mixture Model for Internet Search-Engine Visits. *Journal of Marketing Research* 41(2 May), 206-214.
Zauberman, Gal. 2003. "The Intertemporal Dynamics of Consumer Lock-In." *Journal of Consumer Research*. 30(3 December), 405-19.

Table 1
Timing of the attacks

	Time of Attack*	# users in category at time	# users online at time
FREE			
CNN	Tues. Feb. 8: 7:00 PM–8:50 PM	56	587
Yahoo	Mon. Feb. 7: 1:20 PM–4:20 PM	401	650
ZDNet	Wed. Feb. 9: 6:45 AM–9:45 AM	16	397
SHOPPING			
Amazon	Tues. Feb. 8: 8:00 PM–9:00 PM	38	423
Buy.com	Tues. Feb. 8: 1:50 PM–4:50 PM	88	717
EBay	Tues. Feb. 8: 6:20 PM–7:50 PM	10	375
OTHER			
E*Trade	Wed. Feb. 9: 8:00 AM–9:30 AM	37	168

*All times EST. Source: CNET (Sandoval and Wolverton 2000).

Table 2: Impact of Denial of Service Attacks on Attacked Websites
Utility Maximization/Random Effects Probit Regression Results

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	FREE			SHOPPING			OTHER
Coefficients							
Variable	**CNN**	**Yahoo**	**ZDNet**	**Amazon**	**Buy.com**	**EBay**	**E*Trade**
Treatment group & After the attack	-0.0709	-0.124	-0.264	-2.90	-2.02	-0.0272	0.607
	(0.0218)**	(0.0254)**	(0.142)+	(1.24)*	(1.09)+	(0.0549)**	(0.605)
Days since attack* (Treatment & After)	0.00291	0.00154	0.00773	0.0212	0.0122	-0.00565	-0.0171
	(0.00657)	(0.000768)*	(0.00431)+	(0.0382)	(0.128)	(0.0177)	(0.0163)
Treatment group	-0.425	1.13	0.875	0.0131	12.60	0.0735	3.83
	(0.119)**	(0.0163)**	(0.0783)**	(0.716)	(1.92)**	(0.0823)	(0.252)**
After the attack	0.0552	0.0312	-0.0823	-0.0641	-0.0317	0.0793	-0.0730
	(0.0325)+	(0.00779)**	(0.0323)*	(0.0245)**	(0.0622)	(0.0238)**	(0.0387)+
Chose attacked website last visit	1.18	1.14	1.10	1.02	1.52	0.0613	0.625
	(0.0230)**	(0.00490)**	(0.0216)**	(0.0177)**	(0.0467)**	(0.0158)**	(0.0310)**
Media mention	0.0315	0.00429	-0.0172	-0.0198	0.0133	0.0174	0.0963
	(0.0315)	(0.00450)	(0.0389)	(0.0156)	(0.0634)	(0.0148)	(0.0302)**
Log(bytes uploaded on last visit to non-attacked site)	-0.000240	-0.0248	-0.00843	-0.00925	0.0282	-0.0670	-0.0190
	(0.00734)	(0.00181)**	(0.00753)	(0.00485)+	(0.0112)*	(0.00622)**	(0.00788)*
Log(bytes uploaded on last visit to attacked site)	-0.0344	-0.0276	-0.00604	0.0213	0.0373	-0.00858	-0.0418
	(0.00829)**	(0.00222)**	(0.00694)	(0.00596)**	(0.0148)*	(0.00526)	(0.0117)**
Days since attack	-0.000240	-0.000330	0.00308	-0.000841	-0.00103	-0.00322	0.00187
	(0.000975)	(0.000219)	(0.000987)**	(0.000741)	(0.00181)	(0.000661)**	(0.00115)
Marginal Effects							
Treatment group & After the attack	-0.0382	-0.0390	-0.0783	-0.0511	-0.00769	-0.00961	0.0148
	(0.0118)**	(0.00799)**	(0.0419)+	(0.0219)*	(0.00415)+	(0.0194)**	(0.0147)
Days since attack* (Treatment & After)	0.000157	0.000484	0.00228	0.00373	0.0000463	-0.00199	-0.000417
	(0.000354)	(0.000242)*	(0.00128)+	(0.00675)	(0.000490)	(0.00625)	(0.000396)
Treatment group	-0.0229	0.356	0.259	0.00231	0.0481	0.0259	0.0932
	(0.00642)**	(0.00512)**	(0.0232)**	(0.126)	(0.00733)**	(0.0290)	(0.00613)**
After the attack	0.00296	0.00980	-0.0244	-0.0114	-0.000121	0.0281	-0.00180
	(0.00175)+	(0.00244)**	(0.00958)*	(0.00435)**	(0.000240)	(0.00844)**	(0.000955)+
Chose attacked website last visit	0.161	0.384	0.365	0.264	0.0599	0.0218	0.0310
	(0.00314)**	(0.00166)**	(0.00718)**	(0.00461)**	(0.00184)**	(0.00561)**	(0.00154)**
Media mention	0.00174	0.00135	-0.00507	-0.00349	0.0000512	0.00614	0.00252
	(0.00174)	(0.00141)	(0.0114)	(0.00275)	(0.000240)	(0.00521)	(0.000790)**
Log(bytes uploaded on last visit to non-attacked site)	-1.32E-05	-0.00780	-0.00250	-0.00163	0.000107	-0.0236	-0.000462
	(0.000404)	(0.000568)**	(0.00223)	(0.000856)+	(4.25E-05)*	(0.00219)**	(0.000192)*
Log(bytes uploaded on last visit to attacked site)	-0.00185	-0.00867	-0.00179	0.00377	0.000142	-0.00303	-0.00102
	(0.000447)**	(0.000696)**	(0.00205)	(0.00105)**	(5.61E-05)*	(0.00186)	(0.000285)**
Days since attack	-1.30E-05	-0.000105	0.000913	-0.000148	-3.92e-06	-0.00114	4.55E-05
	(5.28E-05)	(6.97E-05)	(0.000290)**	(0.000131)	(6.89E-06)	(0.000230)**	(2.81E-05)
Observations	106,129	855,370	37,471	69,342	83,414	47,019	154,511
Log likelihood	-13,152	-262,115	-12,591	-21,052	-3,858	-24,621	-10,322

All regressions include a constant. Standard errors in parentheses.
+p<0.10; *p<0.05; **p<0.01

Table 3: Impact of Denial of Service Attacks on Attacked Websites
Utility Maximization Regression Results for Yahoo—Other Specifications

	(1)	(2)	(3)	(4)	(5)	(6)
Variable	**Random Effects (as Table 2)**	**Fixed Effects**	**Random Effects; No decay effect**	**Random Effects; No lagged choice**	**Random Effects; Treatment by visit propensity**	**Random Effects; Treatment relative to rival frequency**
Treatment group & After the attack	-0.124	-0.0873	-0.0739	-0.196	-0.0870	-0.158
	(0.0254)**	(0.0167)**	(0.0162)**	(0.0246)**	(0.0201)**	(0.0248)**
Days since attack* (Treatment & After)	0.00154	-0.000280		0.00306	-0.000359	0.00283
	(0.000768)*	(0.000472)		(0.000705)**	(0.000555)	(0.000744)**
Treatment group	1.13	0.551	0.561	0.0725	1.51	-0.0512
	(0.0163)**	(0.0167)**	(0.0139)**	(0.0140)**	(0.0139)**	(0.0166)**
After the attack	0.0312	0.00320	0.0240	0.0526	0.0323	0.00895
	(0.00779)**	(0.00666)	(0.00512)**	(0.00752)**	(0.00772)**	(0.00739)
Days since attack	-0.000330	0.000489		-0.000890	-9.00E-05	0.000133
	(0.000219)	(0.000189)**		(0.000211)**	(0.000209)	(0.000211)
Marginal Effects of Key Variables						
Treatment group & After the attack	-0.0390	-0.0296	-0.0217	-0.0523	-0.0292	-0.0419
	(0.00799)**	(0.00565)**	(0.00476)**	(0.00654)**	(0.00675)**	(0.00658)**
Days since attack* (Treatment & After)	0.000484	-9.60E-05		0.000816	-0.000121	0.000751
	(0.000242)*	(0.000160)		(0.000188)**	(0.000187)	(0.000198)**
Observations	855,370	816,297	855,370	855,370	855,370	855,370
Log likelihood	-262,115	-318,110	-262,115	-288,011	-262,017	-262,519

All regressions include Chose attacked website last visit, Media mentions, Log(bytes uploaded on last visit to non-attacked site), Log(bytes uploaded on last visit to attacked site), and a constant. Standard errors in parentheses. +p<0.10; *p<0.05; **p<0.01

Table 4: Impact of Denial of Service Attacks on Attacked Websites
Probabilistic Differences and Duration Models[15]

		(1)	(2)	(3)	(4)	(5)	(6)
		General Model	**Marginal Effects of 1 Std. Dev. Change**	**Weighted by total number of visits by household**	**Additional regressors**[16]	**# Visits rather than Market Share**	**Exponential Duration—on days to next visit**
FREE	CNN	-0.208^	-0.00715^	-0.135	-0.115	-25.26	-0.548
		(0.126)		(0.101)	(0.112)	(17.38)	(0.959)
	Yahoo	-0.0540**	-0.00985**	-0.0632**	-0.0529**	-94.14**	-0.551**
		(0.0194)		(0.0184)	(0.0191)	(12.76)	(0.155)
	ZDNet	-0.259^	-0.0154^	-0.500	-0.0125	-44.12**	-0.610
		(0.154)		(0.353)	(0.142)	(7.47)	(0.488)
SHOPPING	Amazon	-0.238	-0.00471	-0.456*	-0.253	6.95	-9.91**
		(0.180)		(0.232)	(0.274)	(35.86)	(1.27)
	Buy.com	-0.521*	-0.00245*	-1.36**	-0.500*	-63.67	-2.36
		(0.239)		(.116)	(0.233)	(61.10)	(4.18)
	EBay	-0.205	-0.0172	-0.231^	-0.0829	-49.88*	-0.105
		(0.134)		(0.120)	(0.109)	(23.24)	(0.385)
OTHER	E*Trade	-0.0244	-0.000560	-0.0291	0.0259	-45.91	1.02
		(0.221)		(0.275)	(0.202)	(32.12)	(1.01)

All regressions have a constant. Standard errors in parentheses. Except col. 2, all #'s are coefficients. +p<0.10; *p<0.05; *p<0.01

[15] Probabilistic differences number of observations: Amazon=1,932, Buy=1,990, CNN=1,544, EBay=572, E*Trade=432, Yahoo=2,479 and ZDNet=944. Duration model number of observations: Amazon=4,178, Buy=417, CNN=3,820, EBay=13,701, E*Trade=1,285, Yahoo=119,273 and ZDNet=4,849.

[16] Regressors include difference in average media mentions, difference in average bytes downloaded from the attacked website, and difference in average bytes downloaded from the attacked website's competitors. Bytes uploaded, pages viewed, and time spent give the same significance results, with less explanatory power.

Table 5: Impact of Denial of Service Attacks on Rival Websites (Switching Cost Identification)
Utility Maximization/Random Effects Probit Regression Results

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	FREE			SHOPPING			OTHER
Variable	**CNN**	**Yahoo**	**ZDNet**	**Amazon**	**Buy.com**	**EBay**	**E*Trade**
Treatment group &	0.687	0.119	0.462	-3.62	-6.45	-1.65	-3.95
After the attack	(0.401)+	(0.0373)**	(0.686)	(1.42)*	(4.04)	(0.748)*	(0.918)**
Days since attack*	-0.0363	-0.00721	-0.0399	0.0844	-0.0644	0.0682	-0.0710
(Treatment & After)	(0.0139)**	(0.00110)**	(0.0258)	(0.0330)*	(0.117)	(0.0272)*	(0.0339)*
Treatment group	0.454	-0.186	-2.04	0.323	6.20	-2.27	-0.427
	(0.205)*	(0.204)	(0.388)**	(0.883)	(1.97)**	(0.363)**	(0.540)
After the attack	-0.167	-0.0124	0.0635	0.806	0.0268	1.17	0.430
	(0.0627)**	(0.0153)	(0.163)	(0.135)**	(0.0704)	(0.5336)*	(0.0425)**
Substitutability proxy	-4.77E-07	-7.40E-07	5.57E-06	5.60E-06	7.01E-07	9.91E-06	1.13E-07
	(4.56E-08)**	(6.20E-08)**	(1.34E-06)**	(7.38E-07)**	(8.01E-07)	(3.99E-06)*	(8.13E-08)
Days since attack	0.00873	0.000330	0.00807	-0.0195	-0.00283	-0.0535	-0.00783
	(0.00199)**	(0.000440)	(0.00555)	(0.00358)**	(0.00198)	(0.0237)*	(0.00133)**
Marginal Effects of Key Variables							
Treatment group &	0.201	0.0467	0.0297	-0.687	-0.723	-0.521	-1.55
After the attack	(0.117)+	(0.0146)**	(0.0441)	(0.269)*	(0.453)	(0.236)*	(0.361)**
Days since attack*	-0.0106	-0.00283	-0.00257	0.0160	-0.00722	0.0216	-0.0279
(Treatment & After)	(0.00407)**	(0.000431)**	(0.00166)	(0.00625)*	(0.0131)	(0.00861)*	(0.0133)*
Observations	21,828	221,842	2,392	5,530	12,310	1,013	36,232
Log likelihood	-4,282	-90,085	-576.4	-1,309	-2,498	-327.5	-10,282

Table 6: Impact of Denial of Service Attacks on Rival Websites (Switching Cost Identification)
Utility Maximization/Random Effects Probit Results using Treatment Relative to Rival Frequency

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	FREE			SHOPPING			OTHER
Variable	**CNN**	**Yahoo**	**ZDNet**	**Amazon**	**Buy.com**	**EBay**	**E*Trade**
Treatment group &	0.539	0.427	0.511	0.377	0.950	-2.00	1.08
After the attack	(0.225)*	(0.0404)**	(0.601)	(0.312)	(0.242)**	(0.558)**	(0.105)**
Days since attack*	-0.00660	-0.00531	-0.0171	-0.00452	-0.000355	0.0725	0.00244
(Treatment & After)	(0.00644)	(0.00116)**	(0.0202)	(0.00898)	(0.00681)	(0.0223)**	(0.00318)
Treatment group	0.853	-1.67	-0.508	-1.76	-1.35	-1.05	-1.91
	(0.107)**	(0.0251)**	(0.292)+	(0.210)**	(0.139)**	(0.245)**	(0.0628)**
After the attack	-0.0493	-0.0988	0.262	0.300	-0.564	1.15	-0.00629
	(0.0710)	(0.0164)**	(0.176)	(0.216)	(0.163)**	(0.394)**	(0.0570)
Substitutability proxy	-2.37E-07	-7.34E-08	3.58E-06	4.12E-06	1.02E-07	-5.16E-06	-6.41E-07
	(4.60E-08)**	(5.79E-08)	(5.43E-06)	(7.39E-07)**	(2.32E-06)	(3.57E-06)	(7.93E-08)**
Days since attack	0.00508	-0.000770	0.00628	-0.00933	-0.00291	-0.0490	-0.00722
	(0.00221)*	(0.000459)+	(0.00630)	(0.00624)	(0.00470)	(0.0184)**	(0.00170)**
Marginal Effects of Key Variables							
Treatment group &	0.195	0.170	0.0573	0.0640	0.242	-0.786	0.430
After the attack	(0.0814)*	(0.0161)**	(0.0673)	(0.0530)	(0.0616)**	(0.219)**	(0.0418)**
Days since attack*	-0.00239	-0.00212	-0.00192	-0.000767	-0.0000905	0.0286	0.000972
(Treatment & After)	(0.00233)	(0.000462)**	(0.00227)	(0.00152)	(0.00173)	(0.00879)**	(0.00127)
Observations	21,828	221,842	2,392	5,530	12,310	1,013	36,232
Log likelihood	-4,265	-89,852	-570.1	-1,299	-2,503	-324.0	-10,202

All regressions include Chose attacked website last visit, Media mentions, Log(bytes uploaded on last visit to non-attacked site), Log(bytes uploaded on last visit to attacked site), and a constant. Standard errors in parentheses. "Rival" refers to the website visited during the attack instead of the attacked website. +p<0.10; *p<0.05; **p<0.01

Table 7: Impact of Denial of Service Attacks on Rival Websites (Switching Cost Identification)
Utility Maximization Regression Results for Yahoo—Other Specifications

	(1)	(2)	(3)	(4)	(5)	(6)
Variable	**Random Effects (as Table 5)**	**Fixed Effects**	**Random Effects**	**Random Effects, Includes Choose Yahoo**	**Random Effects; Treatment by visit propensity**	**Random Effects; Treatment relative to rival frequency (as Table 6)**
Treatment group &	0.119	0.160	0.0425	0.233	0.0153	0.427
After the attack	(0.0373)**	(0.0332)**	(0.0250)+	(0.0331)**	(0.0901)+	(0.0404)**
Days since attack*	-0.00721	-0.00363		-0.00509	-0.00391	-0.00531
(Treatment & After)	(0.00110)**	(0.000941)**		(0.000955)**	(0.000382)**	(0.00116)**
Treatment group	-0.186	-0.818	-0.213	-1.68	-0.376	-1.67
	(0.204)	(0.300)**	(0.0290)**	(0.0209)**	(0.0246)**	(0.0251)**
After the attack	-0.0124	-0.0241	-0.0264	-0.0498	0.446	-0.0988
	(0.0153)	(0.0139)+	(0.0102)**	(0.0147)**	(0.0933)**	(0.0164)**
Substitutability proxy	-7.40E-07	-6.33E-07	-1.23E-06	-1.26E-06	-2.92E-07	-7.34E-08
	(6.20E-08)**	(1.21E-04)**	(5.87E-08)**	(5.43E-08)**	(5.64E-08)**	(5.79E-08)
Days since attack	0.000330	-0.00144		-0.000706	-0.00137	-0.000770
	(0.000440)	(0.000392)**		(0.000415)+	(0.000382)**	(0.000459)+
Marginal Effects of Key Variables						
Treatment group &	0.0467	0.0640	0.0168	0.0824	0.00610	0.170
After the attack	(0.0146)**	(0.0132)**	(0.00987)+	(0.0117)**	(0.0395)+	(0.0161)**
Days since attack*	-0.00283	-0.00145		-0.00180	-0.00155	-0.00212
(Treatment & After)	(0.000431)**	(0.000375)**		(0.000338)**	(0.000151)**	(0.000462)**
Observations	221,842	220,043	221,842	309,413	221,842	221,842
Log likelihood	-90,085	-100,824	-90,120	-109,870	-90,052	-89,852

All regressions include Chose attacked website last visit, Media mentions, Log(bytes uploaded on last visit to non-attacked site), Log(bytes uploaded on last visit to attacked site), and a constant. Standard errors in parentheses. "Rival" refers to the website visited during the attack instead of the attacked website. +p<0.10; *p<0.05; **p<0.01

Table 8: Impact of Denial of Service Attacks on Rival Websites (Switching Cost Identification)
Probabilistic Differences and Duration Models[17]

		(1)	(2)	(3)	(4)	(5)
		General model	**Marginal effects of 1 standard deviation change**	**Weighted by total number of visits**	**With controls for substitutability**	**Exponential Duration Model—on days to next visit**
FREE	CNN	0.442	0.0569	0.487	0.440	0.107
		(0.286)		(0.419)	(0.288)	(0.434)
	Yahoo	0.162**	0.0209**	0.100*	0.162**	0.144**
		(0.0454)		(0.0460)	(0.0453)	(0.0614)
	ZDNet	0.122^	0.0328^	2.35	0.0661	0.0171
		(0.0680)		(1.41)	(0.379)	(0.106)
SHOPPING	Amazon	0.510	0.0452	-1.07	0.612	0.0521
		(0.460)		(1.94)	(0.471)	(0.172)
	Buy.com	0.759	0.0164	1.43	0.768	-8.29**
		(1.31)		(2.21)	(1.32)	(1.21)
	EBay	0.138	0.0514	0.509	0.0582	2.73
		(0.385)		(0.386)	(0.494)	(7.40)
OTHER	E*Trade	-1.48	-0.0280	-0.638	-1.51	0.679**
		(1.64)		(0.736)	(1.66)	(0.117)

All regressions include a constant. Standard errors in parentheses. Except column 2, all numbers are coefficients.
+p<0.10; *p<0.05; **p<0.01

[17] Probabilistic differences number of observations: Amazon=38, Buy=88, CNN=56, EBay=10, E*Trade=37, Yahoo=401 and ZDNet=16. Duration model number of observations: Amazon=13,463, Buy=4,123, CNN=3,783, EBay=414, Yahoo=118,965 and ZDNet=1,276.