

Distribution Agreement

In presenting this thesis or dissertation as a partial fulfillment of the requirements for an advanced degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis or dissertation in whole or in part in all forms of media, now or hereafter known, including display on the world wide web. I understand that I may select some access restrictions as part of the online submission of this thesis or dissertation. I retain all ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Michael R. Hammock

Date

Three Essays in Voluntary Regulation by Firms

By

Michael R. Hammock

Doctor of Philosophy

Economics

Dr. Maria Arbatskaya

Co-Advisor

Dr. Paul H. Rubin

Co-Advisor

Dr. Andrew Francis

Committee Member

Dr. Tilman Klumpp

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the Graduate School

Date

Three Essays in Voluntary Regulation by Firms

By

Michael R. Hammock
B.S., Berry College, 1996
M.S., Texas A&M, 1998

Co-advisor: Maria Arbatskaya, Ph.D
Co-Advisor: Paul H. Rubin, Ph.D
Committee Member: Andrew Francis, Ph.D
Committee Member: Tilman Klumpp, Ph.D

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Economics
2010

Abstract

Three Essays in Voluntary Regulation by Firms

By Michael R. Hammock

Firms sometimes choose to undertake costly actions that are beneficial to their customers or other business partners, but which are not required by regulation. These three chapters examine why businesses might or might not undertake some voluntary actions. Chapter one examines firms' pollution behavior, and concludes that firms do not face an incentive to reduce their unregulated toxic emissions, but that the evidence is consistent with firms using lobbying to permit higher levels of emissions. Chapter two surveys the literature on the economics of information security, finding that while firms may underprovide security (relative to the efficient level), some security problems have been solved, and for others it is unclear that additional policy action is justified. Chapter three examines the role of certification seals in online retail, and the use of such seals to provide consumers with assurances of privacy, quality, and most importantly, security. It finds evidence that security seals correlate with a price premium for online retailers, suggesting that voluntary regulation may be working well in this area.

Three Essays in Voluntary Regulation by Firms

By

Michael R. Hammock
B.S., Berry College, 1996
M.S., Texas A&M, 1998

Co-advisor: Maria Arbatskaya, Ph.D
Co-Advisor: Paul H. Rubin, Ph.D
Committee Member: Andrew Francis, Ph.D
Committee Member: Tilman Klumpp, Ph.D

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Economics
2010

Acknowledgements

I would like to thank Maria Arbatskaya, Paul H. Rubin, Tilman Klumpp, and Andrew Francis for their input on all chapters, and Ujjayant Chakravorty and Jerry Thursby for their input on the first chapter. I am also grateful to Opensecrets.org for their data and support services. All errors or omissions are solely the fault of the author. Special thanks are due to my wife for her patience.

Table of Contents:

	Contents	Page
1	Chapter 1: Lobbying, Political Contributions, and Corporate Emissions: an Empirical Investigation	1
	1.1 Introduction	1
	1.2 Prior Literature	3
	1.3 A Simple Model of Emissions and Political Behavior	8
	1.4 The Data	12
	1.5 Estimation One: Political Influence Allows Emissions	19
	1.6 Estimation Two: Models Based on Damania and Maxwell et al.	22
	1.7 Conclusion	25
	Appendix	28
	References	49
2	Chapter 2: A Review of the Economics of Information Security Literature	51
	2.1 Introduction	51
	2.2 The Problems: What Are They and How Big Are They?	52
	2.3 An Aside: Retail Internet Security Technology	58
	2.4 The Incentive Problems of Information Security	61
	2.5 Improving Security: Private Solutions	66
	2.6 Improving Security: Policy Solutions	71
	2.7 Implications for the Future	77
	2.8 Conclusions	79

	References	80
3	Chapter 3: Do Certification Seals Permit a Price Premium	88
	3.1 Introduction	87
	3.2 Literature	91
	3.3 The Hypothesis To Be Tested	94
	3.4 Data	96
	3.5 Estimation Technique and Results	101
	3.6 Discussion	106
	3.7 Conclusions	108
	References	124

	Tables and Figures	Page
	Figure 1: U.S. Emissions, 1996 to 2000	16
	Table 1.1: Firms in the Sample	28
	Table 1.2: Summary Statistics	33
	Table 1.3: Results for Level of Emissions, Panel Data with Fixed Effects	35
	Table 1.4: Results for Change in Emissions, Panel Data with Fixed Effects	36
	Table 1.5: Results for Level of Emissions, Panel Data with Random Effects	37
	Table 1.6: Results for Level of Emissions (without logs), panel data with Random Effects	39
	Table 1.7: List of Chemicals and Toxic Equivalency Potentials (TEPS)	41

Table 3.1: Variable Definitions	109
Table 3.2: Summary Statistics	113
Table 3.3: Page Source Search Terms	115
Table 3.4: Items and their Product Categories	117
Table 3.5: Regression 1	118
Table 3.6: Regression 2	119
Table 3.7: Regressions 3 and 4	121
Table 3.8: Regressions 5, 6, 7, and 8	122

Chapter 1

Lobbying, Political Contributions, and Corporate Emissions: an Empirical Investigation

Mike Hammock

Abstract:

The relationship between a firm's pollution behavior and its political behavior is analyzed using a novel combination of data sets. Panel data on lobbying, political contributions, emissions, chemical toxicity, and corporate finances yields a simple and intuitive result: Firms that expend more effort on influencing the government also pollute more. Two related theories from the literature on abatement and political influence are also tested, but are not confirmed.

1.1 Introduction:

The relationship between firms' emissions and their political behavior is unclear and cannot be derived a priori. Firms might try to increase emissions to increase the costs of future regulation, weakening the government's incentive to regulate (Damania 2001). Alternatively firms might try to reduce emissions to deter consumers from entering a lobbying game, thereby reducing the likelihood of regulation (Maxwell et al. 2000). The model proposed in this paper suggests that it may be in the interest of firms to produce high emissions, not to reduce the likelihood of regulation, but simply because it may be cheaper to pollute, using lobbying and political contributions to avoid regulation than to incur the costs of abatement. Firms that spend more on political contributions and lobbying can afford to release higher emissions. Rather than focusing

on abatement levels as Damania (2001) and Maxwell et al. (2000) do, this model focuses on the level of pollution, ignoring the firm's choice of whether or not to invest in abatement technology. In the short run this is probably a reasonable assumption, as abatement technologies may be fixed until research and development have had time to create new technologies.

This chapter empirically investigates the relationship between the level of a firm's emissions and the firm's political behavior using a novel set of panel data. The other theories of environmental behavior by firms are also tested, although the data are less well suited to such tests. I find that firms differ significantly in their behavior, with dirtier firms (or more accurately, firms with more toxic emissions) spending more on lobbying and political contributions, controlling for size of the firm and other firm characteristics. This suggests that firms find it cheaper to substitute lobbying expenditures and political contributions for emissions reductions. That is, it seems to be cheaper for firms in this data set to "buy" their way out of potential regulation than to deter it through voluntary pre-emptive emissions reductions. It does not seem to be the case that firms increase their emissions in order to deter regulation. Changes in emissions do not appear to be related to political behavior.

The first section of the paper reviews the existing literatures on voluntary abatement and lobbying expenditures. Section 2 provides a simple model to motivate the empirical analysis. Section 3 introduces the data and the many challenges in working with it. The fourth section presents the results of testing the model provided in this paper, and the fifth section presents the results from testing versions of Damania's (2001) and

Maxwell et al.'s (2000) hypotheses. Section 6 summarizes the results, discusses objections to them, and explains their economic significance.

1.2 Prior Literature

The empirical literature on the relationship between firms' environmental behavior and their political behavior is small. John Maxwell, Thomas Lyon, and Steven Hackett (2000) study toxicity-weighted emissions in the United States at the state level, and find that states with the highest reductions in unregulated chemicals from 1988 to 1992 are also those with the highest per capita membership in environmental organizations such as the Sierra Club. They also find that states that had high per capita membership in environmental organizations and that started the period with high toxicity of emissions (i.e., an interaction term) had higher reductions in emissions of unregulated chemicals. Their results are very strong, with an R-squared of 0.97—stunningly high for any cross-sectional regression. I have some concern regarding the chemicals they chose to study (the seventeen “unregulated” chemicals they selected were in fact chosen for regulation by Congress under the 1990 Amendment to the Clean Air Act, although the form of regulation would not be decided for several years, and this fact cannot explain the variation in reductions across states), but it is difficult to argue with the strength of their results. Their data strongly supports the hypothesis that firms reduce emissions to reduce the threat of regulation. I have adopted some of their methodology in this paper, particularly the use of toxicity weights as a method of aggregating emissions of diverse chemicals. Nonetheless their data is concerned with behavior at the state level, while I

am interested in the behavior of individual firms. I will test a version of their theory, along with a version of Damania's theory, in the Estimation section below.

Khanna and Anton (2004) look at the Environmental Management Systems (EMSs) adopted by firms, and use two creative measures of the regulatory threat the firms face: The number of superfund sites for which a firm has been named a potentially responsible party, and the ratio of certain hazardous air pollutants (HAPs) to overall (or "on-site") releases. Their results vary depending on the specification, but it is fair to say that firms with more Superfund sites are more likely to implement more EMS processes. The ratio of HAPs to on-site releases does not appear to be consistently significant. They have therefore found some evidence that firms undertake some "green" activities in response to possible regulatory threats.¹ See also Khanna (2001) for a survey of the literature on voluntary environmental actions by firms.

Neither of these papers tries to empirically and explicitly link corporate environmentalism to attempts to influence government policy. That is, neither paper investigates the political efforts of firms undertaking these emissions reductions or EMSs. Damania, Fredriksson, and Osang (2005) develop an industry-level model which suggests that pollution intensive industries should have larger levels of political contributions. They suggest that firms can sustain cooperation in political contributions when facing environmental regulation because punishment (in the form of an end to cooperation) in other political areas—particularly trade—is available. Similarly, an end to cooperation in political contributions for environmental regulation can be used as a threat to sustain political contributions in other areas. They do not model the policy maker's decision

¹ Other papers, such as Arora and Cason (1995) investigate why firms participate in voluntary emissions reductions programs, such as the EPA's 33/50 program, but do not attempt to determine if firms are trying to influence policy. They find that participation is determined by size and a desire for public recognition.

explicitly (as is done in the model in this paper), focusing instead on the relationship between pollution intensity and political contributions. The model predicts that firms in pollution-intense industries should have higher levels of political contributions. They find support for this hypothesis using data from the 1980s. However, they ignore actual lobbying (as opposed to political contributions—a distinction explained below), as such data is not available for that period. They also consider only the five or six² criteria pollutants (carbon monoxide, volatile organic compounds, nitrogen oxides, sulfur dioxide, fine particulate matter less than ten microns, lead, and total suspended particulate matter) for their measure of pollution intensity. These chemicals are now regulated in varying degrees.

Canton (2007) models the interaction between polluting industries, government, environmentalists, and “eco-industry”. Eco-industry deals with preventing, reducing, or correcting environmental damage. The effect of the battle between these interest groups on the level of a pollution tax is ambiguous.

This brings us to the relatively new literature on lobbying, and the well-developed literature on political contributions. At this point it is useful to define the terms *lobbying* and *political contributions*, and by doing so emphasize how they differ. Economists often use “lobbying” to mean any effort to influence government policy. Sometimes we even describe the donation of funds to political campaigns as “lobbying” (Gawande 1998). Yet it is important to make a distinction between hiring a lobbyist to talk to a congressperson about environmental regulations, and giving money to a politician’s campaign. *Political Contributions* are the funds donated by individuals, corporations, or

² There are actually six EPA criteria pollutants, but the paper refers only to five. The source of the discrepancy is unclear.

other entities to political parties or politicians (or their campaigns or political action committees). *Lobbying* is any attempt to influence policymakers through some form of communication (excluding political contributions). A company that gives \$2,000 to Congressman Smith's campaign is making a political contribution. A company that hires a lobbyist to spend an hour a week briefing Congressman Smith on the firm's position on the costs of environmental regulation is engaged in lobbying.

The empirical literature on lobbying is small, mainly because of the paucity of data. Older studies primarily rely on survey data, and attempt to tie them with political contributions. A good survey of the literature is presented in Tripathi et al., 2002. Summarizing their survey briefly, Gais and Walker (1991) find that most interest groups surveyed found lobbying important, but few found political contributions important. Berry (1977) and Wright (1989) find that political contributions are fairly uncommon among groups engaging in lobbying, whereas Nownes and Freeman (1999) and Scholtzman and Tierney (1986) find slightly higher rates of contributions among groups engaging in lobbying. Langbein (1986) actually measures the time spent by ninety-two representatives in meetings with lobbyists, and finds that representatives that spent more time in such meetings raised more through their Political Action Committees. (de Figueiredo and Kim 2004) examine the circumstances in which firms might use employees for lobbying, or hire outside lobbyists, finding that firms are more likely to use employees when the issue is very firm specific or involves sensitive information.

Political contribution data has been available for a longer period of time, and available in higher quality than lobbying data. There is therefore a better developed literature on the subject. Smith's (1995) survey and critique of the literature finds that

over thirty-five studies have been done on the relationship between campaign contributions and the voting behavior of senators and representatives. The results are diverse, with eight finding no significant effects, sixteen reporting significant effects, and twelve with mixed results (for example, the effect of contributions on voting may vary from issue to issue, or from congressperson to congressperson, or from year to year). Less effort has been spent on *who gives* contributions and *why* (that is, why some groups give and others do not).

(Tripathi, Ansolabehere et al. 2002) is worth discussing in some detail both because of the novelty of the results, and because they use the same source of political data used for this paper. They make use of lobbying data collected by the Clerk of the House of Representatives and the Secretary of the Senate (the data will be described in detail below), and combine it with political contribution data (they focus on PACs, the largest destination for contributions), giving us the best view yet of the interaction between lobbying and political contributions. The results relevant to this paper can be summarized as follows:

- Lobbying expenditures on average make up almost ninety two percent of interest group expenditures; political contributions are dwarfed by lobbying expenditure.
- Over seventy percent of expenditures were made by groups with positive lobbying *and* political contribution expenditures. Few groups spent money on only one or the other.
- Lobbying expenditures and political contributions are positively correlated.

- When the groups are divided into different types of organizations (corporations, trade and professional associations, issue and ideological groups, and labor unions) and studied separately, it becomes clear that different groups pursue different strategies. Of particular importance to this paper is the strategy pursued by corporations; they spend the most on lobbying relative to contributions of any group—roughly two dollars in additional lobbying for every additional dollar in contributions.

Overall their results suggest that corporations pursue an access strategy.

Contributions are used to “get the foot in the door,” making lobbying possible and effective. Lobbying expenditure and political contributions appear to be complements in achieving political influence. This is in contrast with ideological groups or “issue goal” groups, who pursue electoral strategies. They spend less on lobbying, and carefully time and structure their contributions to re-elect friendly politicians. These results have another implication for the many studies of the effects of political contributions: They may be wrong-headed due to their exclusion of lobbying expenditures.

1.3 A Simple Model of Emissions and Political Behavior:

Two players, the government and a monopoly firm, attempt to maximize social welfare and profit, respectively, over a three stage game. The firm chooses output and lobbying, while the government chooses a pollution tax. Social welfare is the sum of the area under the linear demand curve, less the damage caused by pollution (to which the government can be made less sensitive by lobbying) and the cost of lobbying, which is a

deadweight loss to society. The pollution tax revenue does not show up in the social welfare function as it is a transfer. This results in the following social welfare function:

$$W = aQ - \frac{1}{2}Q^2 - \frac{(\theta Q - L)^2}{2} - L \quad (1)$$

where

a is a demand parameter (the intercept).

Q is the monopolists's output level.

θ is the pollution intensity of the firm's output, so that total emissions is θQ .

And $\frac{(\theta Q - L)^2}{2}$ is the damage caused by pollution, which (from the government's

perspective) is mitigated by political effort, L .³ It must be assumed that $\theta > \frac{L}{Q}$, or the

damage function would be decreasing in output.

In the first stage the firm chooses how much to invest in political effort. In the second stage the government sets the pollution tax. The firm then produces its profit-maximizing output in the third stage. Production costs are assumed away for simplicity. Solving the game with backward induction, we begin with the third stage.

³ This model is intentionally vague regarding how or why lobbying affects the government, assuming only that if the policymakers act counter to the intent of lobbyists, they are somehow worse off. This could be because they anticipate a reduction in future political contributions, or because they are concerned that they may be making a mistake in their estimates of social welfare (as corporate lobbyists are sure to tell them). Lobbying must have some effect or firms would not do it.

Stage 3:

The firm maximizes profit by choosing output:

$$\pi = (a - Q)Q - t\theta Q - L \quad (2)$$

Where t is the tax per unit of pollution. The optimal output level is

$$Q^* = \frac{a - t\theta}{2} \quad (3)$$

Output is decreasing in taxes and pollution intensity.

Stage 2:

The government chooses the socially optimal level of output:

$$\frac{dW}{dt} = a - Q - Q\theta^2 + L\theta = 0$$

$$L\theta + a = Q + Q\theta^2$$

$$Q^E = \frac{L\theta + a}{(1 + \theta^2)} \quad (4)$$

The government can find the tax by setting the efficient level of output equal to the profit-maximizing level of output, which gives us

$$t = \frac{a}{\theta} - 2 \frac{L\theta + a}{\theta(1 + \theta^2)} \quad (5)$$

Stage 1:

We substitute (5) and (3) back into (2) to find the firm's optimal choice of L (its best response function). Taking the derivative of the resulting function with respect to L , solving for L , and discarding the root which results in negative lobbying gives the solution:

$$L^* = \frac{\theta^2 + \sqrt{6a\theta^5 + \theta^4 + 12a\theta^3 + 6a\theta}}{3\theta^4 + 6\theta^2 + 3} \quad (6)$$

This can be used to give us the SPNE values for output and the tax.

$$Q^* = \frac{3a\theta^4 + \theta^3 + 6a\theta^2 + 3a + \theta\sqrt{6a\theta^5 + \theta^4 + 12a\theta^3 + 6a\theta}}{3(\theta^2 + 1)^3} \quad (7)$$

$$t^* = \frac{a}{\theta} - 2 \frac{\left(\frac{\theta^2 + \sqrt{6a\theta^5 + \theta^4 + 12a\theta^3 + 6a\theta}}{3\theta^4 + 6\theta^2 + 3} \right) \theta + a}{\theta(1 + \theta)^2} \quad (8)$$

The central question is “should firms that emit pollution lobby more or less?”

Equilibrium emissions are

$$\theta Q^* = \theta \frac{a - t\theta}{2} \quad (9)$$

Substituting the optimal tax:

$$\theta Q^* = \theta \frac{a - \left(\frac{a}{\theta} - 2 \frac{L\theta + a}{\theta(1 + \theta^2)} \right)}{2} = \theta \frac{L\theta + a}{\theta^2 + 1}$$

Emissions and lobbying are positively related. Note also that (9) shows that, other things equal, a larger firm (i.e., one facing a larger demand parameter, a , produces larger emissions.

The primary testable hypothesis is therefore demonstrated: firms with higher lobbying have higher emissions. This result differs from both Damania’s (2001) and Hackett et al.’s results. It is similar to Damania (2005), except that paper suggests a positive correlation between political contributions and pollution intensity at the *industry* level.

The assumption of monopoly in this model is useful in that it eliminates free-rider problems in lobbying. The same pressure to lobby would exist in a market with more than one firm, but it would be undermined by the temptation to allow competing firms to incur the costs of lobbying, while enjoying the benefits of lower pollution taxes. The assumption of monopoly complicates matters somewhat, in that a negative tax (a subsidy) is efficient when the pollution intensity, θ , is low. This is because of the standard inefficiently low level of monopoly output. The firm continues to lobby for a more negative tax (a larger subsidy) in this case, although it is not of empirical interest.

1.4 The Data:

The availability of political contribution data, lobbying expenditure data, and toxic emissions data makes possible new kinds of analysis. By studying the relationship between these variables, we may be able to determine what kind of political strategy firms are pursuing. In the previous section I proposed that firms may simply prefer to pollute at will, fighting regulation using political contributions and lobbying alone. If this is the case, then firms with higher emissions should have higher expenditures on political contributions and lobbying. If firms are using emissions reductions as a political tool to deter consumers from entering a lobbying game (Maxwell, Lyon et al. 2000) then they will not need to spend as much on political contributions and lobbying expenditures. We should find that firms with significant reductions in emissions have lower lobbying and political contribution expenditures. Finally, if firms are attempting to be extremely dirty in order to raise the costs of future regulation (Damania 2001) we should find that firms that spend more on lobbying will undertake less abatement.

Testing these theories required the collection and correction of a great deal of data. Three primary sources of data were used: The EPA's Toxics Release Inventory (TRI), Opensecrets.org's lobbying and political contribution data, and financial data from Hoovers (and occasionally other sources when Hoovers lacked information about a particular firm).

The Toxics Release Inventory is collected annually by the Environmental Protection Agency (EPA). Any facility (factory, refinery, gas station, etc.) belonging to one of twenty-five SIC code groups with ten or more full-time employees that emits more than a certain threshold of over 581⁴ different chemicals must report those emissions, as well as the form the emissions take (air release, water release, or off-site transfer). Reporting facilities also report information about their environmental management practices (such as recycling), contact information, their parent company's name and Dun and Bradstreet number, and other data. The EPA makes TRI data freely available from 1996 onward via their website⁵.

There is, however, a serious drawback to using this data to study emissions at the level of the parent company: The reported information on parent companies is poorly organized. Parent company names are sometimes outdated; perhaps the company has changed names but the employee in charge of reporting recorded the old name. Sometimes a subsidiary is identified instead of the ultimate parent company. Parent company names are often listed in several different ways; for example BP might be listed as BP, BP INC., BP INCORPORATED, or even BP/AMOCO. The parent company names are often misspelled, or, even worse, not reported at all. Sometimes other data,

⁴ There are technically up to 650 chemicals listed, depending on how one categorizes related chemicals. Chemicals have been added to the list over time due to legislative and regulatory changes.

⁵ www.epa.gov/tri/

such as the D&B number, or the address of the facility, can be used to find the correct parent company. Obviously this makes finding aggregate corporate emissions difficult. Anyone considering using TRI data to look at corporate emissions should be aware that they face the long, tedious task of correcting thousands of mistaken entries. The aggregation of emissions data can be automated, but the correction of parent company names must be done by hand. For this reason I have restricted my analysis to 150 firms⁶. More firms can be added, but it is costly to do so. The list of firms is contained in Table 1.1 in the Appendix.

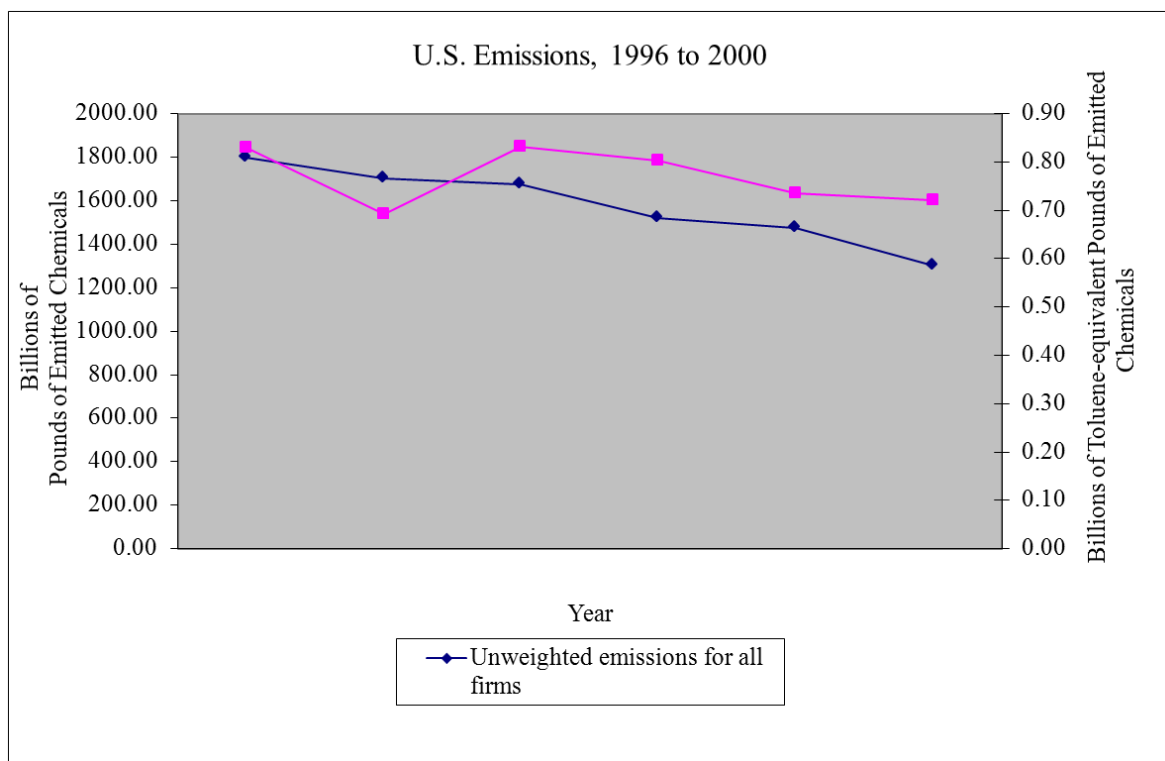
Another problem remains once the corporate aggregation problem has been solved. One cannot simply add the emissions of different chemicals released in different ways. That is, a pound of phenol released in the air added to a pound of ethylbenzene released in the water does not result in any meaningful measure. Maxwell, Lyon, et al (2000) solved this problem using toxicity weights from scorecard.org. I use an updated version of the weights called Toluene Equivalency Potentials, or TEPS. Each chemical has several TEPS values that tell how toxic that chemical is relative to toluene. For example, if the water release TEPS value for anilazine is 110, then a pound of anilazine released in water is 110 times more toxic than a pound of toluene released in water. By multiplying each chemical by the appropriate TEPS and summing over all the chemicals for each firm, we arrive at a measure of a firm's total toxicity of emissions. For the purposes of this study 173 chemicals were selected and total corporate emissions were calculated. Again following (Maxwell, Lyon et al. 2000), non-cancer risks scores were used because of the relative lack of data on cancer risks. Many TRI chemical releases

⁶ Initially, that is. As I add variables, some of which are unavailable for some firms, the sample size drops to 116 firms, for a total of 429 observations (some firms do not have data for all four years for various reasons). The STATA programs used to aggregate the emissions data are available on request.

were omitted, either because they were regulated or because no TEPS figures were available. It is possible that this biases the results, although it is hard to know in what direction. It is unclear how firms or policymakers would measure the effect of chemicals whose toxicity is unknown. I also calculate unweighted emissions for each firm to check the robustness of the results (even though the usefulness of such a number is doubtful).

Figure 1 depicts total emissions of all facilities from 1996 to 2000, the period of our sample. The diamond series in represents unweighted air and water emissions of the 183 unregulated chemicals in the sample (that is, adding dissimilar chemicals, resulting in a measure without a clear interpretation). The square series represents weighted air and water emissions (the toluene-pound equivalent of all emitted chemicals).

Figure 1



Both weighted and unweighted emissions generally move downward over the period, although there is an inexplicable seventeen percent dip in the weighted emissions from 1996 to 1997. There were no regulatory changes in 1997, so the cause of the dip is unknown. Weighted emissions then return to their previous level before declining. There is therefore some evidence that firms are voluntarily reducing emissions, at least at a national level. Another explanation could be a shift in production (and pollution) overseas (where environmental regulations are less strict). However, manufacturing output is rising over this period—indeed, it has been rising almost every year for fifty years. Finally, this could simply be an unintentional side effect of improvements in technology. New production technologies may simply produce less waste, including pollution, as a result of improved efficiency.

Some unregulated chemicals were excluded from these figures and all subsequent analysis. Specifically, Persistent, Bioaccumulative, and Toxic (PBT) chemicals and some other chemicals were subject to a reduction in reporting thresholds in 2000. Including these chemicals would make it impossible to compare year 2000 emissions to previous years. Including them would be sufficient to make weighted emissions climb from 1996 to 1999, while unweighted emissions still fall. Apparently firms are using more of these chemicals, even as they reduce usage of others. It may be worthwhile to investigate these specific chemicals in greater detail, particularly as they are apparently of particular interest to policymakers, and therefore possible candidates for regulation. Nonetheless they are excluded from the present analysis.

The second source of data is the website opesecrets.org, which is operated by the Center for Responsive Politics (CRP), a non-profit, non-partisan research group. CRP

organizes publicly available data on political contributions and lobbying expenditures. The Federal Election Commission requires that contributions from individuals, Political action Committees, and other organizations be reported. It makes scans of the reporting forms available for free on its website, but they are not aggregated or well-organized. Similarly, the Clerk of the House and the Secretary of the Senate have collected data on lobbying expenditures since 1997. Any organization spending more than \$20,000 in a year, either on in-house lobbyists or outside lobbying contractors, must report those expenditures. This does mean that organizations that spend less than \$20,000 on lobbying do not appear in the data, but this should not be a serious problem. \$20,000 is, in the world of lobbying, an insignificant, inconsequential expenditure. Scans of the reporting forms can be viewed on the website of the Secretary of the Senate.

Scans of thousands of documents are a hassle to deal with, but opensecrets.org organizes these documents for us. They aggregate and organize political contributions and lobbying expenditures, making it mostly possible to find out how much a particular organization has spent on lobbying or donated to political campaigns. I say “mostly” because the opensecrets.org data is subject to the same kinds of errors from which the EPA’s TRI data suffers—misidentification of subsidiaries, typos, unnoticed name changes, and so on. The opensecrets.org data is nonetheless in far better shape than the EPA’s data, and correcting its problems is not as time consuming. I have data on total political contributions made by each firm in my sample from 1996 to 2000. I also asked Opensecrets.org for data on contributions to members of the Senate Environment and Public Works Committee, hoping that perhaps firms that were more interested in influence over environmental policy would spend more effort on the congressional

committee most focused on such policy. Lobbying data from 1997 to 2000 was also obtained for each firm in my sample. A few firms had either no political contributions or lobbying expenditures to report. Some firms, especially textile firms, had both zero political contributions and zero lobbying expenditures.

Firms may pollute a great deal because they have lobbied hard and feel that it is safe to do so. But a more likely and direct cause of high emissions is simply high production. Firms that produce a great deal of output produce more emissions than firms that produce little output. Of course, with so many industries and kinds of output it is impossible to measure output itself. This brings us to the third source of data. Again following Maxwell, Lyon et al. (2000), who use value of shipments in each state as a measure of state output, I use revenue as a measure of each firm's output. Net Sales data would be preferable, but it is difficult to collect for some firms. Revenue is itself difficult to collect for a few firms, particularly in the textile industry, where many prominent firms are private and do not publicly report financial data. Financial data simply could not be obtained at all for some firms, and as a result they are excluded from regressions with revenue as an explanatory variable. In a few cases data was obtained from Thompson One Banker, corporate websites, or brief references in online business articles. Dollar values were deflated to 1996 dollars using the CPI.

Dummy variables for firm characteristics were also collected. Eight dummies represent the various industries of the firms, and a ninth dummy indicates whether the firm is publicly traded. These dummies are ultimately unused because I will be using fixed effects (random effects results are also reported, with dummies included).

Table 1.2 presents summary statistics for the variables. Because all the variables are highly skewed to the right, and because no relationships emerge between the variables in levels, I will use logs in the actual estimation. Logged variables and dummy variables are not included in the summary statistics.

1.5 Estimation One: Political Influence Allows Emissions

Several different models are estimated due to uncertainty over the correct specification, and to test the different hypotheses. The theory section above suggested a simple result: Firms with high emissions may avoid regulation by spending money on political contributions and lobbying. Larger firms are likely to produce higher emissions. This is not a surprising or counterintuitive result, but it has not, to my knowledge, been tested, and the literature on corporate emissions has lately focused on voluntary abatement, rather than simple lobbying in order to continue emitting. Of course, a firm's level of emissions is not likely to be determined simply by their political strategy. Industry or even firm characteristics (such as technology and production processes) may affect the level of emissions as well⁷. The relationship between political behavior and emissions is not necessarily causal in one direction, either—perhaps firms produce a level of emissions and choose their political strategy accordingly, or their political strategy allows them to emit a certain amount. I am interested in the correlation; do firms that spend more on political effort emit more? If so, this suggests a relationship between their emissions and their political behavior. The estimated models use panel data regression

⁷ In casual conversation with a lobbyist I was informed that the nature of the firm's production would have by far the largest impact on a firm's emissions. He argued that firms would only reduce emissions as a result of their natural capital cycle. When old, expensive equipment wore out, firms would replace it with newer equipment, which would naturally be cleaner. This begs the question of why the new equipment is cleaner, rather than being dirtier and cheaper. Perhaps more efficient new equipment is necessarily cleaner.

with fixed effects⁸. The panel is unbalanced due to the entry and exit of some firms from the data due to mergers and acquisitions. The starting equation to be estimated is:

$$\ln(Emissions_{it}) = \beta_1 \ln(Lobbying_{it}) + \beta_2 Contributions_{it} + \beta_3 DirectContributions_{it} + \beta_4 revenue_{it} + \beta_5 dummy1997_t + \beta_6 dummy1998_t + \beta_7 dummy1999_t + \alpha_i + \eta_{it}$$

Table 1.3 presents the primary results. Log of weighted emissions were used first as the dependent variable, followed by log of unweighted emissions. Note that the coefficients represent elasticities. In addition to a model with all the independent variables, I also estimated “refined” regressions omitting variables with p-values higher than 0.4. The results differ depending on the independent variable used, but some results remain relatively unchanged. In particular, the log of lobbying and the log of real revenue are always significant at the 5% level or better. Curiously, political contributions directed to members of the Environment and Public Works committee are significant at the 10% level in the unweighted emissions regression, but not when weighted emissions are used. This is difficult to explain (although at such a low significance level, it is probably not worth much attention). It might suggest that congresspersons are not sophisticated enough to be interested in toxicity, rather than raw emissions, but this does not explain why overall political contributions are significant in *both* the weighted and unweighted regressions. It is hard to believe that members of the committee are less sophisticated than senators and representatives in general. In fact I was surprised to find the directed contributions variable significant in any of the regressions; I was expecting corporations to find it easier to work through congresspersons that have company

⁸ Random Effects results are available in the Appendix in table 1.5. A Hausman test confirmed that Fixed Effects are the way to go. If one really must have a higher R-squared one might be more interested in the Random Effects, but the results are otherwise very similar; the coefficients have the same sign and are of similar magnitudes. Random Effects results are reported in tables 1.5 and 1.6 in the appendix.

facilities in their district, rather than particular committee members. Perhaps some omitted variable is biasing the coefficients⁹. The models were further refined by leaving out variables that are not significant at the 10% level, but this does not change the results appreciably. Note that the 1997 year dummy variable is significant in three of the regressions, and negative in all of them. This makes sense for the weighted data, given the dip in 1997 emissions in the unweighted data.

The general picture presented by the results is consistent with the theory that firms use political influence to deter or influence environmental regulation. Firms with higher lobbying expenditures have higher emissions, and firms with higher political contributions have higher emissions, *ceteris paribus*. It may be the case that contributions directed to the Senate Committee on Environment and Public Works are also associated with higher emissions. The strength of the result should not be overstated, however. While the F statistic is high for all regressions, R-squared is not. Furthermore these results do not prove causation; they are merely consistent with the theory. The results cannot tell us whether firms are more concerned about regulators acting on the basis of their emissions or the toxicity of their emissions. Some anecdotal evidence supports the latter, as in the case of the PBT reporting requirement changes mentioned earlier. An EPA that tightens reporting requirements for especially toxic chemicals that are emitted in increasing amounts is an EPA that is more likely to regulate on the basis of toxicity.

⁹ There are surely several important omitted variables; the level a firm's emissions are not determined simply by their output and political strategy. In part this is addressed by fixed effects and the year dummy variables, but other factors may be important. For example, firms might have low emissions because they have more advanced and efficient processes; a measure of a firm's technology would therefore be useful. A firm might have low emissions because it is trying to attract "green consumers"; if so, there might be a relationship between the firm's advertising expenditures and its emissions. Such variables are hard to obtain reliably for many firms, although future iterations of this paper may include them. I also tried various interaction terms using industry dummies in the fixed effect regression, but they were not significant.

I also calculated the number of reporting facilities for each firm in each year, and estimated separate regressions including this as an explanatory variable. The results are not reported here for brevity, but the coefficient of the number of facilities was significant and positive. That is, firms with more facilities in a given year had higher emissions, *ceteris paribus*. Inclusion of this variable did not affect any of the other coefficients, nor did it much improve overall explanatory power of the regressions.

1.6 Estimation Two: Models Based on Damania and Maxwell et al.

Let us consider a variant of Damania's (2001) theory. Recall that Damania suggests that firms may use pollution as a commitment mechanism. Underinvestment in abatement technology signals the government that stricter regulation will reduce profits and political contributions. The government values these contributions, so the government is less likely to regulate. Damania suggests that the best tests of his theory would look at the effects of firm behavior on policy, but with infrequent changes in federal environmental regulation, particularly over the period during which data is available, it is difficult to do this. Damania's model furthermore assumes homogeneous firms, so that all firms respond to regulatory threats in the same way.

Clearly the model as originally conceived cannot be fully tested with this data; we do not have changes in regulation and homogeneous firms do not exist. I nonetheless believe that one of the model's central propositions can be tested, if we are willing to make a reasonable assumption. Damania's Proposition 2 says that if abatement costs are high enough, lobbying lowers the level of investment in pollution technology. That is, underinvestment in technology is a credible commitment device. Put simply, if Damania

is correct, firms that spend more on lobbying will do less cleaning up. Such firms' emissions will fall by a smaller amount.

Suppose that firms' behavior differs according to their characteristics. Perhaps some firms have low abatement costs, for example. Then it seems reasonable to expect firms that exert more political effort to do the least cleanup, and firms with low political effort to do the most cleanup. Firms that are using underinvestment in abatement technology as a commitment device need to lobby, while firms that clean up do not. This hypothesis is testable with the data already described. Damania almost suggests this himself in his discussion of anecdotal evidence. He mentions that industries that are older and use older technology seem to be more successful at gaining trade protection. If there is variation across industries then perhaps there can be similar variation within industries. It is important to note that this is a theory of *abatement*, or the *change* in the level of emissions. The previous estimation was based on a theory about the *level* of emissions.

The theoretical model used in Maxwell et al. (2000) reaches a different conclusion. In that model firms (a concentrated interest group) can deter consumers (a dispersed interest group) from entering a lobbying game by increasing abatement and increasing lobbying expenditure¹⁰. That is, lobbying and abatement are both tools in achieving political outcomes. Lobbying influences politicians, while abatement influences consumers. By doing more lobbying and more abatement firms induce consumers to reduce their lobbying expenditures, thereby avoiding regulation (or lessening its severity). Maxwell et al. assume homogeneous firms, but again we can

¹⁰ Note that Maxwell et al. use the term "lobbying" to mean political influence or pressure in general. I will refer their theory using the term "lobbying", but I also include political contributions in the estimation.

make the reasonable assumption that firms interested in influencing the political process will do more abatement and more lobbying, while firms that are not interested in influencing the political process will do less abatement and less lobbying.¹¹

Damania and Maxwell et al. (or our slightly modified versions of them) therefore present us with two conflicting predictions: Firms trying to influence environmental regulation will abate less and exert more political influence (Damania) or abate more and exert more political influence (Maxwell et al.). We can test these hypotheses with the same data used in the previous section. Instead of looking at the level of emissions, we consider the change in emissions. The basic equation to be estimated is

$$\Delta Emissions_{it} = \beta_1 \ln(Lobbying_{it}) + \beta_2 Contributions_{it} + \beta_3 DirectContributions_{it} + \beta_4 Revenue_{it} + \beta_5 dummy1997_t + \beta_6 dummy1998_t + \beta_7 dummy1999_t + \alpha_i + \eta_{it}$$

Table 1.4 presents regressions testing this proposition using four different dependent variables: Change in Weighted Emissions, Change in Unweighted Emissions, Percent Change in Weighted Emissions, and Percent Change in Unweighted Emissions. I have included all the explanatory variables from before.

The results are clear: There is no relationship between a firm's political behavior and its increase or decrease in emissions. One cannot even reject the hypothesis that all the coefficients are equal to zero. The results are robust; they remain with random effects, lagged variables, levels instead of logs for the independent variables, and so on.¹²

If the result is to be believed, firms neither use emissions reductions and political

¹¹ See Maxwell et al.'s Figure 2, which depicts the firms' and consumers' reaction curves, and the equilibria with and without abatement. Abatement makes lobbying useful to the firm, because it weakens the lobbying effort by consumers.

¹² It is possible to get a positive and significant coefficient on the log of real lobbying expenditures by restricting the analysis to only those firms with weighted emissions reductions (some firms increase emissions in some years). All other variables are not significant, however, and the regression only explains 0.7% of the variation in abatement. The result does not occur with unweighted emissions.

influence as tools to deter political opponents, nor use political influence and emissions reductions as a commitment device. Of course, the lack of a result is not necessarily convincing. It could occur for several reasons. For example, if some firms are pursuing Damania's strategy, while others pursue Maxwell et al.'s strategy, the relationships may be impossible to extract without another variable to distinguish between firms pursuing the different strategies. No such variable is obvious to me. Other possible problems with this and the previous estimation are discussed below.

1.7 Conclusion

The two sets of results presented above suggest that firms do not engage in strategic manipulation of their emissions and political effort. They may instead use political effort as a tool, by itself, to allow the continued production of high levels of emissions.

To put the results of the first estimation (Table 1.3) in context, consider a typical firm. Using the means from Table 1.2, and the refined unweighted regression from Table 1.3, a firm that spent an additional 1% on lobbying—around \$12,319—emits an additional 0.185%, or around 2,238 pounds of emissions. From the refined weighted regression, that same 1% increase in lobbying by an average firm in 2000 leads to a 0.286% increase in weighted emissions, which is the equivalent of about 3,139,315 pounds of additional toluene—a significant increase.

Yet the analysis is incomplete, suffering from several problems. First, the results cannot explain the nationwide drop in unweighted emissions over the sample period. Some process must be driving this reduction. Maxwell et al.'s state-level analysis

suggests it is due to the presence of strong environmental groups in some states; the data in this paper is more national and ill-suited to studying behavior at the state level. It might be worthwhile, however, to re-test their state-level results this using this broader and more recent set of chemical data. It is also possible that firms are reducing emissions in an attempt to attract environmentally conscious consumers. The inclusion of advertising expenditures might control for this (as firms that reduce emissions might spend more effort trying to advertise their “green” status), but advertising expenditures are difficult to collect for most firms. Also, many of these firms are far up the supply chain; it is doubtful that consumers even know who they are. Perhaps the suppliers of final goods apply pressure to them.

A second problem is that I have not attempted to incorporate the possibility that firms are trying to harm their competitors (rather than all firms pursuing a similar policy, i.e. less regulation) by means of political effort or changes in emissions. It is difficult to see how to address this problem; we do not know exactly for what purpose firms spent money on lobbying and political contributions (if we did, this analysis would be unnecessary), and I know of no variable that could tell us more than we already know.

Third, and perhaps most importantly, I have not considered the effect and efforts of trade organizations. Firms often coordinate their political effort via trade organizations, and sometimes (as in the case of the American Chemistry Council’s Responsible Care initiative) work together to reduce emissions. It is likely that there is some coordination of this type occurring that is not reflected in the data. Although we can look up the political contributions and lobbying expenditures made by trade organizations, we cannot assign these expenditures to particular firms (contributions to

trade organizations from firms are confidential, and some organizations do not even release a list of members).

This leaves a great deal of room for additional research. It may be worthwhile to repeat this analysis at the industry level, although the resulting small sample size may make this difficult. Adding new firms from additional industries might also improve the analysis. Use of net sales instead of revenue might better approximate a firm's output (although such data is even more difficult to obtain than revenue data for firms that are privately owned). More generally, the relationship between the political behavior of firms (in terms of lobbying expenditures and political contributions) could be related to many different kinds of policies.

The policy implications of these results are unclear. The results do not imply that regulation is ineffective, or that firms should not be regulated. They merely suggest that firms actively resist regulation using political means. Firms spending more on political contributions and lobbying produce more pollution, but firms that spend more on political contributions and lobbying do not, on average, abate more or less.

Appendix:

Table 1.1
Firms in the Sample

Number	Firm Name	Industry Name ¹³
1	Connell L.P.	Energy/National Resources
2	Enron Corporation	Energy/National Resources
3	Southern Company	Energy/National Resources
4	Mobil	Energy/National Resources
5	Exxon	Energy/National Resources
6	ExxonMobil	Energy/National Resources
7	BP	Energy/National Resources
8	Amoco	Energy/National Resources
9	BP/Amoco(BP)	Energy/National Resources
10	Dominion Resources	Energy/National Resources
11	Chevron	Energy/National Resources
12	Dynegy Corp.	Energy/National Resources
13	Entergy Corporation	Energy/National Resources
14	Koch Industries	Energy/National Resources
15	El Paso Energy	Energy/National Resources
16	TXU Corporation	Energy/National Resources
17	Edison International	Energy/National Resources
18	Exelon Corporation/PECO	Energy/National Resources
19	FirstEnergy Corporation	Energy/National Resources
20	USX Corporation	Energy/National Resources
21	Reliant Energy	Energy/National Resources
22	FPL Group	Energy/National Resources
23	PG&E Corporation	Energy/National Resources
24	Anadarko Petroleum	Energy/National Resources
25	Texaco Corporation	Energy/National Resources
26	Royal Dutch/Shell Group	Energy/National Resources
27	Phillips Petroleum Company	Energy/National Resources
28	Conagra Foods	Agribusiness
29	Tyson Foods Incorporated	Agribusiness
30	Perdue Incorporated	Agribusiness
31	UST Inc.	Agribusiness
32	International Paper	Agribusiness
33	Flo-Sun Inc.	Agribusiness
34	Archers Daniels Midland	Agribusiness

¹³ Opensecrets.org bases its industry classification on SIC codes.

35	Yucaipa Companies	Agribusiness
36	PepsiCo Inc.	Agribusiness
37	Dairy Farmers of America Inc.	Agribusiness
38	Connell Company	Agribusiness
39	American Crystal Sugar Company	Agribusiness
40	Services Group of America	Agribusiness
41	Georgia-Pacific Corporation	Agribusiness
42	Pilgrim's Pride Corporation	Agribusiness
43	Ocean Spray Cranberries Inc.	Agribusiness
44	Lockheed Martin	Defense
45	General Dynamics	Defense
46	Northrop Grumman	Defense
47	Raytheon Co.	Defense
	Science Applications International	
48	Corporation	Defense
49	United Technologies Corporation	Defense
50	Honeywell International	Defense
51	DRS Technologies	Defense
52	BAE Systems PLC	Defense
53	United Defense	Defense
54	Boeing Company	Defense
55	Coca-Cola Co.	Food and Beverage
56	General Motors	Transportation
57	Chrysler Corporation	Transportation
58	Daimler-Benz	Transportation
59	Daimler Chrysler	Transportation
60	Ford Motor Company	Transportation
61	Honda Motor Company	Transportation
62	Nissan Motor Company	Transportation
63	Toyota Motor Corporation	Transportation
64	Northwest Airlines	Transportation
65	Delta Airlines	Transportation
66	Continental Airlines	Transportation
		Chemical and Related
67	Procter & Gamble	Manufacturing
		Chemical and Related
68	Goodyear Tire & Rubber	Manufacturing
		Chemical and Related
69	Ashland Inc.	Manufacturing
70	Lyondell Chemical	Chemical and Related

	Manufacturing
	Chemical and Related
71 Millennium Chemicals Inc.	Manufacturing
	Chemical and Related
72 Dow Chemical	Manufacturing
	Chemical and Related
73 Air Products & Chemicals Inc.	Manufacturing
	Chemical and Related
74 Dupont Co.	Manufacturing
	Chemical and Related
75 Plastech Engineered Products	Manufacturing
	Chemical and Related
76 SC Johnson & Son	Manufacturing
	Chemical and Related
77 Contran Corp.	Manufacturing
	Chemical and Related
78 PVS Chemicals	Manufacturing
	Chemical and Related
79 Bridgestone Americas	Manufacturing
	Chemical and Related
80 Eastman Chemicals	Manufacturing
	Chemical and Related
81 Praxair Inc.	Manufacturing
	Chemical and Related
82 BASF Corporation	Manufacturing
	Chemical and Related
83 Plastipak Packaging	Manufacturing
	Chemical and Related
84 PPG Industries	Manufacturing
	Chemical and Related
85 Ethyl Corporation	Manufacturing
	Chemical and Related
86 Philipp Brothers Chemicals	Manufacturing
	Chemical and Related
87 Atlantic Richfield	Manufacturing
	Chemical and Related
88 FMC Corporation	Manufacturing
	Chemical and Related
89 Monsanto Co	Manufacturing
90 Harris Chemical Group	Chemical and Related

	Manufacturing
	Chemical and Related
91 Dial Corporation	Manufacturing
	Chemical and Related
92 WR Grace & Co	Manufacturing
	Chemical and Related
93 ICI Americas Inc.	Manufacturing
	Chemical and Related
94 Turtle Wax	Manufacturing
	Chemical and Related
95 Hermann Companies	Manufacturing
	Chemical and Related
96 Sid Richardson Carbon	Manufacturing
	Chemical and Related
97 Hercules Inc.	Manufacturing
	Chemical and Related
98 IMC Global Inc.	Manufacturing
99 Springs Industries	Textiles
100 Standard Textile Co.	Textiles
101 Milliken & Co.	Textiles
102 Weave Corporation	Textiles
103 Levy Group	Textiles
104 Peter J. Solomon Co.	Textiles
105 Shaw Industries	Textiles
106 Gibbs International	Textiles
107 Atkins & Pearce	Textiles
108 Hobbs Bonded Fibers	Textiles
109 Api Industries	Textiles
110 Burlington Industries	Textiles
111 Cheraw Yarn Mills	Textiles
112 Prodesco Inc.	Textiles
113 SL Gilbert Co	Textiles
114 Fabrica International	Textiles
115 Dixie Group	Textiles
116 A-One Carpet	Textiles
117 Kentucky Derby Hosiery	Textiles
118 Patrick Yarns	Textiles
119 Powell Corporation	Textiles
120 Guilford Mills	Textiles
121 Card-Monroe Corporation	Textiles

122	American House Spinning Inc.	Textiles
123	Harry Miller Co.	Textiles
124	Duro Industries	Textiles
125	Mayo Yarns	Textiles
126	Beaulieu of America	Textiles
127	NTC Group	Textiles
128	Mayfair Mills	Textiles
129	Bayer Corp	Pharmaceutical Manufacturing
130	Ivax Corp.	Pharmaceutical Manufacturing
131	Agvar Chemicals	Pharmaceutical Manufacturing
132	Glaxo Wellcome Inc.	Pharmaceutical Manufacturing
133	Eli Lilly & Co.	Pharmaceutical Manufacturing
134	Pfizer Inc.	Pharmaceutical Manufacturing
135	Bristol-Myers Squibb	Pharmaceutical Manufacturing
136	Schering-Plough Corp.	Pharmaceutical Manufacturing
137	American Home Products	Pharmaceutical Manufacturing
138	Roche Group	Pharmaceutical Manufacturing
139	Rhone Poulenc Inc.	Pharmaceutical Manufacturing
140	Zeneca Inc.	Pharmaceutical Manufacturing
141	Merck & Co.	Pharmaceutical Manufacturing
142	SmithKline Beecham	Pharmaceutical Manufacturing
143	Baxter International	Pharmaceutical Manufacturing
144	United States Surgical Corp.	Pharmaceutical Manufacturing
145	AMGEN Inc.	Pharmaceutical Manufacturing
146	Abbott Laboratories	Pharmaceutical Manufacturing
147	Johnson & Johnson	Pharmaceutical Manufacturing
148	Novartis	Pharmaceutical Manufacturing
		Chemical and Related
149	Ciba Specialty Chemicals	Manufacturing
150	Pharmacia & Upjohn	Pharmaceutical Manufacturing

Table 1.2
Summary Statistics

Year	Variable	Definition	Mean	SD	Minimum	Maximum
1996	Unweighted Emissions	Total pounds of 173 unregulated chemicals emitted by 150 companies	1.39	3.82	0	30.10
1997			1.33	3.93	0	31.00
1998			1.12	2.91	0	20.80
1999			1.07	2.95	0	22.60
2000			1.21	4.44	0	42.50
1996	Weighted Emissions	Toluene pound equivalent of chemical toxicity for emitted chemicals	585	3,249	0	30,300
1997			1,005	5,989	0	66,700
1998			1,297	5,768	0	48,400
1999			972	3,989	0	30,107
2000			1,098	4,623	0	31,000
1996	Lobbying	Lobbying Expenditures over \$20,000 per year, in 1996 dollars, adjusted for inflation using CPI	NA	NA	NA	NA
1997			1.23	2.05	0	10.36
1998			1.23	2.05	0	13.29
1999			1.24	1.97	0	11.01
2000			1.23	1.96	0	10.19
1996	Contributions	Total political contributions, in 1996 dollars, adjusted for inflation using CPI	198,396	258,598	0	1,303,837
1997			114,577	146,381	0	758,862
1998			166,820	199,298	0	850,992
1999			166,115	215,066	0	1,077,660
2000			271,233	350,771	0	1,569,663
1996	Directed Contributions	Total political contributions to members of the Senate Environment and Public Works Committee, in 1996 dollars,	3,458	5,517	0	30,000
1997			3,336	6,268	0	44,431
1998			2,405	3,487	0	18,963
1999			2,292	4,514	0	35,599

2000		adjusted for inflation using CPI	2,279	3,729	0	17,585
1996	Revenue	Total revenue in millions of	18,301.18	28,935.79	3.20	158,015.00
1997		1996 dollars, adjusted for	18,377.36	28,814.55	5.57	162,711.65
1998		inflation using CPI	17,840.63	27,782.65	3.18	148,960.62
1999			19,231.05	31,345.50	6.69	157,624.23
2000			22,699.05	37,053.43	11.66	187,772.49

Table 1.3
Results for Level of Emissions, Panel Data with Fixed Effects¹⁴

Independent Variable	Dependent Variable							
	ln(Weighted Emission)				ln(Unweighted Emissions)			
	Full Model		Refined		Full Model		Refined	
ln(Real Lobbying)	0.283	***	0.286	***	.180	***	0.185	***
	(3.64)		(3.73)		(3.57)		(3.72)	
ln(Real Contributions)	0.262	**	0.256	**	0.138	*	0.129	*
	(2.22)		(2.23)		(1.81)		(1.74)	
ln(Real Directed Contributions)	0.092		0.094		0.106	*	0.112	*
	(.407)		(.97)		(1.66)		(1.59)	
ln(Real Revenue)	2.237	***	2.199	***	1.551	***	1.488	***
	(3.11)		(3.19)		(3.33)		(3.32)	
Year 1997 dummy	-0.977	*	-1.060	**	-0.391		-0.537	**
	(-1.81)		(-2.57)		(-1.12)		(-1.63)	
Year 1998 dummy	0.076		--		.119		--	
	(0.15)				(0.35)			
Year 1999 dummy	0.151		--		-0.282		--	
	(0.29)				(0.85)			
Constant	-12.183	*	-11.764	*	-7.683	*	-6.975	*
	(-1.90)		(-1.95)		(-1.85)		(-2.00)	
Overall R ²	0.261		0.261		0.286		0.284	
Number of firms	116							
Number of observations	429							

¹⁴ Numbers in parentheses are t-statistics. ***indicates significance at the 1% level, ** at the 5% level, and * at the 10% level.

Table 1.4
Results for Change in Emissions, Panel Data with Fixed Effects¹⁵

Independent Variable	Dependent Variable			
	Change in Weighted Emissions		Change in Unweighted Emissions	
	Actual	Percent	Actual	Percent
ln(Real Lobbying)	1100625 (0.01)	-3149.756 (-0.48)	91.76481 (0.00)	-.2047332 (-0.98)
ln(Real Contributions)	1.43e+07 (0.07)	1729.453 (0.16)	-11973.29 (-0.18)	.1190418 (0.34)
ln(Real Directed Contributions)	4787602 (0.03)	-86.001 (-0.01)	3174.44 (0.58)	.182022 (0.74)
ln(Real Revenue)	3.86e+08 (0.29)	21115.780 (0.34)	90218.42 (0.22)	-2.826669 (-1.44)
Year 1997 dummy	6.14e+08 (0.62)	66863.660 (1.62)	-263733.9 (-0.85)	.3204913 (0.25)
Year 1998 dummy	-2.20e+08 (-0.23)	11561.760 (0.28)	-532984.1 * (-1.74)	-.8206415 (-0.62)
Year 1999 dummy	-4.85e+08 (-0.51)	10957.530 (0.28)	-299125.5 (-1.01)	.3023339 (0.24)
Constant	-3.58e+09 (-0.31)	-183033.600 (-0.31)	-652910.6 (-0.18)	27.11595 (1.46)
Overall R ²	0.0005	0.0013	0.0043	0.0013
Number of firms	116	102	116	102
Number of observations	424	333	424	333

¹⁵ T-statistics are as in table 1.3. Some firms were lost when using percent changes because of zeros in the denominator of the dependent variable.

Table 1.5
Results for Level of Emissions, Panel Data with Random Effects¹⁶

Independent Variable	Dependent Variable							
	ln(Weighted Emission)				ln(Unweighted Emissions)			
	Full Model		Refined		Full Model		Refined	
ln(Real Lobbying)	0.201	***	0.202	***	0.138	***	0.143	***
	(2.91)		(2.96)		(3.05)		(3.19)	
ln(Real Contributions)	0.199	**	0.195	**	0.108		.0097	
	(2.00)		(2.00)		(1.63)		(1.50)	
ln(Real Directed Contributions)	0.112		0.115		0.107	***	0.113	*
	(1.24)		(1.29)		(1.80)		(1.94)	
ln(Real Revenue)	2.297	***	2.253	***	1.864	***	1.872	***
	(6.14)		(6.55)		(7.28)		(7.93)	
Year 1997 dummy	-1.056	**	-1.139	***	-0.348		-0.52	**
	(-2.06)		(-2.82)		(-1.05)		(-1.99)	
Year 1998 dummy	.0069				0.177			
	(0.13)				(0.54)			
Year 1999 dummy	0.155				0.328			
	(0.31)				(1.00)			
Energy/Natural	11.168	**	11.199	**	8.168	**	8.135	**

¹⁶ Numbers in parentheses are t-statistics. ***indicates significance at the 1% level, ** at the 5% level, and * at the 10% level.

Resource	(2.08)		(2.11)		(2.16)		(2.18)
Agribusiness	10.477 **		10.587 *		9.954 ***		9.842 ***
	(1.91)		(1.95)		(2.57)		(2.58)
Defense	8.715		8.719		6.106		6.071
	(1.58)		(1.60)		(1.87)		(1.58)
Textiles	12.509 **		12.644 **		10.929 ***		10.723 ***
	(0.030)		(2.23)		(2.69)		(2.69)
Pharmaceutical	8.379		8.349		7.412 *		7.419 **
	(1.55)		(1.56)		(1.95)		(1.97)
Transportation	6.397		6.434		5.002		4.988
	(1.16)		(1.18)		(1.28)		(1.30)
Chemical	14.88473 ***		14.896 ***		12.079 ***		12.029 ***
	(2.76)		(2.80)		(3.18)		(3.21)
Privately Owned	14.885				-0.403		
	(0.29)				(-0.34)		
Constant	-22.221 ***		-21.687 ***		-18.509 ***		-18.392 ***
	(-3.50)		(-3.55)		(-4.17)		(-4.30)
Overall R ²	0.396		0.396		0.457		0.456
Number of firms	116		116		116		116
Number of observations	429		429		429		429

Table 1.6
Results for Level of Emissions (without logs), Panel Data with Random Effects¹⁷

Independent Variable	Dependent Variable			
	Weighted Emission		Unweighted Emissions	
	Full Model	Refined	Full Model	Refined
Real Lobbying	426.515 ** (198.233)	385.541 *** (148.019)	0.149 (0.092)	0.152 * (0.091)
Real Contributions	1035.876 (1554.391)		0.927 (0.72)	
Real Directed Contributions	-33596.36 (56917.67)		23.576 (24.108)	
Real Revenue	-8951.644 (17117.96)		25.505 ** (10.285)	23.338 ** (9.044)
Year 1997 dummy	6.16x10 ⁸ (6.61x10 ⁸)		468224.5 * (2.78x10 ⁶)	394382 * (2.06x10 ⁵)
Year 1998 dummy	5.50x10 ⁸ (6.10x10 ⁸)		129472.1 (254293.6)	
Year 1999 dummy	7.86x10 ⁷ (6.10x10 ⁸)		50292.18 (253734.7)	
Energy/Natural Resource	2.97x10 ⁹ (4.75x10 ⁹)	3.37x10 ⁹ *** (1.07x10 ⁹)	1431614 (3474538)	1495966 * (840902)
Agribusiness	1.76x10 ⁹ (4.84x10 ⁹)	2.20x10 ⁹ * (1.31x10 ⁹)	5707030 (3543698)	5720253 *** (1107567)
Defense	-6.90x10 ⁸ 4.88x10 ⁸		60238.65 (3563823)	

¹⁷ Numbers in parentheses are t-statistics. ***indicates significance at the 1% level, ** at the 5% level, and * at the 10% level.

Textiles	1.21x10 ⁹ (5.06x10 ⁹)	1.64x10 ⁹ (1.31x10 ⁹)	2273056 (3692043)		
Pharmaceutical	-7.93x10 ⁸ (4.80x10 ⁹)		122298.1 (3499352)		
Transportation	2.77x10 ⁹ (4.96x10 ⁹)	2.93x10 ⁹ *	-476964.3 (3606884)		
Chemical	1.15x10 ⁹ (4.76x10 ⁹)	1.66x10 ⁹ (1.05x10 ⁹)	2795394 (3477591)	2795235 *** (875384)	
Privately Owned	-9.86x10 ⁸ (1.41x10 ⁹)	-7.88x10 ⁸ (9.73x10 ⁸)	-2340259 ** (1030249)	-2354051 ** (1010165)	
Constant	-7.25x10 ⁸ 4.72x10 ⁹	-9.02x10 ⁸ (8.14x10 ⁸)	-1141145 (3424621)	-1053319 (629348)	
Overall R ²	.081	0.0885	0.221	0.220	
Number of firms	116	150	116	116	
Number of observations	431	570	431	431	

Table 1.7: List of Chemicals and Toxic Equivalency Potentials (TEPS)		
Chemical Name	Noncancer Air	
	Toxicity Weight	Noncancer Water Toxicity Weight
1,1,1,2-TETRACHLOROETHANE	190	17
1,1,2,2-TETRACHLOROETHANE	7.7	6.2
1,1,2-TRICHLOROETHANE	15	32
1,1-DICHLOROETHANE	14	14
1,1-DICHLOROETHYLENE	6.3	34
1,1-DIMETHYL HYDRAZINE	710	330
1,2,3-TRICHLOROPROPANE	85	110
1,2,4,5-TETRACHLOROBENZOL	25000	44000
1,2,4-TRICHLOROBENZENE	23	160
1,2,4-TRIMETHYLBENZENE	2.6	630
1,2-DIBROMOETHANE	3100	2600
1,2-DICHLOROBENZENE	22	25
1,2-DICHLOROETHANE	14	15
1,2-DICHLOROETHYLENE	7.7	20
1,2-DICHLOROPROPANE	470	550
1,2-TRANS-DICHLOROETHYLENE	1	4.4
1,3-BUTADIENE	0.91	33
1,3-DICHLOROBENZENE	14	16
1,3-DICHLOROPROPENE (MIXED ISOMERS)	11	88
1,4-DICHLOROBENZENE	6.1	3.4
1,4-DIOXANE	0.028	0.088
1-BUTYL CHLORIDE	1.4	1.9
1-CHLORO-1,1-DIFLUOROETHANE	5.9	0.051
1-METHYL-2-NITROBENZENE	2.6	2.1
1-METHYL-3-NITROBENZENE	93	110
2,3,4,6-TETRACHLOROPHENOL	57	110
2,4,5-T	110	9.4
2,4,5-TRICHLOROPHENOL	11	13
2,4,6-TRICHLOROPHENOL	21	0.4
2,4,6-TRINITROPHENOL	12000	1400
2,4,6-TRINITROTOLUENE	390	5.8
2,4-D	32	2.2
2,4-DB	130	13

2,4-DICHLOROPHENOL	46	0.26
2,4-DIMETHYLPHENOL	0.25	1.7
2,4-DINITROPHENOL	160	15
2,4-DINITROTOLUENE	120	1.8
2,4-DP	140	58
2,6-DIMETHYLPHENOL	39	740
2,6-DINITROTOLUENE	190	1.8
2-CHLOR-1,3-BUTADIENE	3.9	41
2-CHLOROPHENOL	20	100
2-CHLOROPROPANE	32	37
2-METHYL-1-PROPANOL	0.27	0.066
2-METHYL-2-PROPENOIC ACID, ETHYL ESTER	0.47	2
2-NITROPROPANE	2.4	22
2-PHENYLPHENOL	0.016	1.4
4,4'-ISOPROPYLIDENEDIPHENOL	3.2	0.74
4,4'-METHYLENEDIANILINE	0.56	0.093
4,6-DINITRO-O-CRESOL	3400	110
4-NITROPHENOL	6.9	8.8
ABAMECTIN	3100	60
ACENAPHTHENE	0.13	4.9
ACEPHATE	250	50
ACETALDEHYDE	2.9	8.1
ACETONE	0.27	0.17
ACETONITRILE	120	52
ACETOPHENONE	5.7	1.4
ACROLEIN	1600	8200
ACRYLAMIDE	2100	49
ACRYLIC ACID	23	0.28
ACRYLONITRILE	26	30
ALDICARB	680	1500
ALDRIN	280000	4000000
ALLYL ALCOHOL	1.3	1.7
ALLYL CHLORIDE	29	71
ALPHA-LINDANE	60	180
ALUMINUM	23000	18
AMMONIA	7.5	0.044
ANILAZINE	1900	110
ANILINE	30	100
ANTHRACENE	0.027	0.015

ANTIMONY	14000	2800
ANTIMONY COMPOUNDS	14000	2800
AROCLOR 1016	3600	380000
AROCLOR 1254	4000000	12000000
ARSENIC	160000	39000
ARSENIC (ORGANIC OR INORGANIC COMPOUNDS)	160000	39000
ATRAZINE	28	0.03
AZINPHOS-METHYL	110	13
BARIUM	720	95
BARIUM COMPOUNDS	720	95
BAYTHION (PHOXIM/VOLATON)	26	110
BENOMYL	3.3	0.8
BENTAZON	1100	3000
BENZENETHIOL	7600	28000
BENZIDINE	90	10
BENZOIC ACID	0.021	0.0039
BENZYL BUTYL PHTHALATE	4.1	0.14
BENZYL CHLORIDE	18	2.7
BERYLLIUM	46000	1100
BERYLLIUM COMPOUNDS	46000	1100
BETA-LINDANE	2400	3900
BIFENTHRIN	190	500
BIPHENYL	0.5	6.4
BIS(2-CHLOROETHYL) ETHER	2.5	6.2
BIS(2-ETHYLHEXYL)PHTHALATE	35	15
BIS(TRIBUTYLTIN) OXIDE	2100	19000
BROMOXYNIL	60	21
CADMIUM COMPOUNDS	3700000	270000
CAMPHECHLOR	3200	4100
CAPTAFOL	110	350
CAPTAN	0.077	0.0062
CARBARYL	0.0022	0.78
CARBENDAZIM	82	28
CARBOFURAN	430	120
CARBON DISULFIDE	3.5	4.7
CARBON MONOXIDE	0.27	
CHLORDANE	65000	340000
CHLORFENVINFOS	450	350
CHLOROACETIC ACID	370	3.2

CHLOROBENZENE	2.1	11
CHLORODIBROMOMETHANE	420	380
CHLORODIFLUOROMETHANE	11	0.082
CHLOROETHANE	0.15	0.15
CHLOROMETHANE	460	260
CHLOROPROPHAM	6.8	2.2
CHLOROTHALONIL	16	1.1
CHLORPYRIFOS	210	1200
CHROMIUM COMPOUNDS	4800	520
CIS-1,2-DICHLOROETHYLENE	24	36
CIS-1,3-DICHLOROPROPENE	13	94
COBALT	60000	130
COBALT COMPOUNDS	60000	130
COPPER	21000	13000
COPPER COMPOUNDS	21000	13000
COUMAPHOS	780	1900
CUMENE	0.23	0.64
CYANAZINE	510	110
CYCLOHEXANE	0.022	0.31
CYCLOHEXANONE	0.016	0.012
CYPERMETHRIN	1500	340
CYROMAZINE	170	74
DDT	55000	120000
DELTAMETHRIN (DECA-)	60	2.3
DEMETON	16000	1500
DIAZINON	2300	1900
DIBUTYL PHTHALATE	15	3.4
DICAMBA	37	8.5
DICHLOROBENZENE (MIXED ISOMERS)	18	19
DICHLOROBROMOMETHANE	1100	810
DICHLORODIFLUOROMETHANE	20	16
DICHLORVOS	190	200
DICOFOL	4300	13000
DIELDRIN	120000	810000
DIETHANOLAMINE	150	3.2
DIETHYL ETHER	0.13	0.53
DIETHYL PHTHALATE	0.56	0.58
DIMETHOATE	1200	1100
DIMETHYL PHTHALATE	0.047	0.0034

DIMETHYLAMINE	13	14
DINITROBUTYL PHENOL	1200	1300
DI-N-OCTYL PHTHALATE	30000	320000
DIPHENYLAMINE	6.6	26
DISULFOTON	8500	8400
DIURON	740	240
ENDOSULFAN	6.9	42
ENDRIN	9000	69000
EPICHLOROHYDRIN	1300	470
ETHOPROP	28000	28000
ETHYL ACETATE	0.091	0.035
ETHYL ACRYLATE	0.47	1.1
ETHYL DIPROPYLTHIOCARBAMATE	1.1	3.7
ETHYLBENZENE	0.25	0.6
ETHYLENE GLYCOL	0.18	0.0077
ETHYLENE GLYCOL MONOETHYL		
ETHER	0.72	0.14
ETHYLENE GLYCOL MONOMETHYL		
ETHER	2.7	34
ETHYLENE OXIDE	1500	700
ETHYLENE THIOUREA	1800	780
FENITROTHION	930	230
FENTHION	5900	27000
FLUORANTHENE	16	15
FLUORENE	2.6	31
FOLPET	5.6	0.046
FORMALDEHYDE	3.6	0.39
FORMIC ACID	0.13	0.0035
FREON 113	22	21
FURAN	26	59
GAMMA-LINDANE	2900	9100
GLYPHOSATE	36	270
HEPTACHLOR EPOXIDE	5800	650000
HEXACHLORO-1,3-BUTADIENE	11000	60000
HEXACHLOROCYCLOPENTADIENE	37	210
HEXACHLOROETHANE	15000	13000
HYDRAZINE	110	260
HYDROCHLORIC ACID	24	0.32
HYDROFLUORIC ACID	7.1	
HYDROGEN SULFIDE	0.038	18

HYDROQUINONE	7.8	0.003
IPIODIONE	28	0.96
ISOPHORONE	0.0061	0.3
ISOPROPYL ALCOHOL	0.0088	0.0069
LEAD COMPOUNDS	1100000	82000
LINURON	210	400
MALATHION	22	14
MALEIC ANHYDRIDE	42	0.000008
MANGANESE	6000	6.9
MANGANESE COMPOUNDS	6000	6.9
M-CRESOL	2.7	1.1
M-DINITROBENZENE	8400	120000
MECOPROP	820	26
METHACRYLONITRILE	510	1100
METHANOL	0.18	0.03
METHOMYL	46	40
METHOXONE	1800	120
METHYL ACETATE	0.082	0.029
METHYL ACRYLATE	0.25	0.51
METHYL BROMIDE	9200	5100
METHYL METHACRYLATE	0.1	1.4
METHYL PARATHION	1100	3600
METHYL TERT-BUTYL ETHER	0.068	0.27
METHYLENE BROMIDE	230	240
METOLACHLOR	9	1.9
METRIBUZIN	12	14
MEVINPHOS	880	100
MOLYBDENUM	24000	7000
M-PHENYLENEDIAMINE	34	17
M-XYLENE	0.12	0.68
N,N-DIMETHYLANILINE	3.6	7.5
NAPHTHALENE	9.6	33
N-BUTYL ALCOHOL	0.71	0.26
N-HEXANE	0.46	13
NICKEL COMPOUNDS	6200	50
NITRIC ACID	4.2	
NITROBENZENE	26	200
NITROGEN DIOXIDE	4.3	0.017
NITROGLYCERIN	1.2	0.64
O-ANISIDINE	25	34

O-CRESOL	3.8	0.68
O-DINITROBENZENE	1700	440
O-NITROANILINE	400	670
OXAMYL	38	1.3
OXYDEMETON METHYL	1800	330
O-XYLENE	0.21	0.8
OZONE	4.4	
PARATHION	200	60
P-CHLOROANILINE	4.5	8.5
P-CRESOL	4.1	0.088
P-DINITROBENZENE	490	510
PENTACHLOROPHENOL	61	0.25
PERMETHRIN	53	94
PHENOL	0.11	0.0047
PHOSGENE	68000	190
PHOSPHORIC ACID	31	
PHTHALIC ANHYDRIDE	12	0.000085
PRIMICARB	36	0.24
PM 10	2.9	
PM 2.5	33	
P-PHENYLENEDIAMINE	0.31	0.052
PRONAMIDE	23	18
PROPACHLOR	69	3
PROPOXUR	28	17
PROPYLENE	0.0053	0.056
PROPYLENE OXIDE	77	46
P-XYLENE	0.2	0.8
PYRAZOPHOS	130	79
PYRENE	2.1	0.45
PYRIDINE	140	15
QUINTOZENE	2800	2800
S,S,S-TRIBUTYLTRITHIOPHOSPHATE	43000	190000
SEC-BUTYL ALCOHOL	0.45	0.2
SELENIUM	16000	3100
SELENIUM COMPOUNDS	16000	3100
SILVER	3200	890
SILVER COMPOUNDS	3200	890
SIMAZINE	200	22
STANNANE, ACETOXYTRIPHENYL	2100	1200
STYRENE	0.024	0.59

STYRENE OXIDE	20	8
SULFATES (1)	9.8	
SULFUR DIOXIDE	6	0.00093
TERT-BUTYL ALCOHOL	4.8	4.8
THALLIUM	24000000	5400000
THIRAM	97	2.6
TIN	77	0.047
TOLCLOFOS-METHYL (RIZOLEX)	43	37
TRANS-1,3-DICHLOROPROPENE	7.6	92
TRIALATE	500	1400
TRIAZOFOS	700	590
TRIBROMOMETHANE	530	540
TRICHLORFON	320	13
TRICHLOROFLUOROMETHANE	49	46
TRIETHYLAMINE	3.4	1.7
TRIPHENYLTIN CHLORIDE	2100	1100
VINYL ACETATE	1.4	1
VINYL BROMIDE	13	73
VINYL CHLORIDE	82	7300
ZINC	370	27
ZINC COMPOUNDS	370	27
ZINEB	13	3.6

References:

- Berry, J. M. (1977). *Lobbying for the People: The Political Behavior of Public Interest Groups*. Princeton, NJ: Princeton University Press.
- Canton, J. (2007). "Redealing the Cards: How the Presence of an Eco-Industry Modifies the political Economy of Environmental Policies," Working Papers 2007.25, Fondazione Eni Enrico Mattei
- Damania, R., P. Frederiksson, P., and T. Osang (2005). "Polluters and Collective Action: Theory and Evidence," *Southern Economic Journal* 72(1): 167-185.
- Damania, R. (2001). "When the Weak Win: The Role of Investment in Environmental Lobbying," *Journal of Environmental Economics and Management* 42(1): 1.
- de Figueiredo, J. M. P. and J. Kim (2004). "When Do Firms Hire Lobbyists? The Organization of Lobbying at the Federal Communications Commission," *Industrial and Corporate Change* 13(6): 883-900.
- Gais, T. and J. Walker (1991). "Pathways to Influence in American Politics," In *Mobilizing Interest Groups in America*. Ann Arbor: University of Michigan Press, 103-121.
- Gawande, K. (1998). "Stigler-Olson Lobbying Behavior in Protectionist Industries: Evidence from the Lobbying Power Function," *Journal of Economic Behavior and Organization* 35(4): 477-499.
- Khanna, M. (2001). "Non-Mandatory Approaches to Environmental Protection," *Journal of Economic Surveys* 15(3): 291-324.

- Khanna, M., and W. Anton (2004). "Incentives for environmental self-regulation and implications for environmental performance," *Journal of Environmental Economics and Management* 48(1): 632-654.
- Maxwell, J., T. Lyon, and S. Hackett (2000). "Self-Regulation and Social Welfare: The Political Economy of Corporate Environmentalism," *Journal of Law and Economics* 43(2): 583.
- Nownes, A., and P. Freeman (1999). "Interest Group Activity in the States," *Journal of Politics* 60: 86-112.
- Scholtzman, K. and J. Tierney (1986). *Organized Interests and American Democracy*. New York: Harper Collins.
- Smith, R. (1995). "Interest Group Influence in the U.S. Congress," *Legislative Studies Quarterly* 20 (1), 89-139.
- Tripathi, M., S. Ansolabehere, and J. Snyder (2002). "Are PAC Contributions and Lobbying Linked? New Evidence from the 1995 Lobby Disclosure Act," *Business and Politics* 4(2): 131-155.
- Wright, J. (1989). "PAC Contributions, Lobbying, and Representatives," *Journal of Politics* 51: 713-729.

Chapter 2

A Review of the Economics of Information Security Literature

Mike Hammock

Abstract:

In the last ten years economists have become interested in the role of online security in promoting online commerce. This paper reviews the literature, with a focus on the role of incentives in creating and solving security problems, as well as discussion of the scale of the problem, and implications for the future of the internet, including cloud computing.

2.1 Introduction:

In his 2000 book on information security, after spending several chapters explaining the technical aspects of information security, Bruce Schneier wrote “People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems”. This is where economists come in: Economists are interested in how incentives shape human behavior. With an understanding of the incentives of both the attackers and defenders of information security, economists hope to make the internet a safer place, thereby increasing the number of transactions that take place there.

Information security is not the same as online privacy. “Privacy” refers to the protection of personal information by refusing to distribute it to a third party *willingly*. So, for example, an online store promises not to sell your email and physical address in order to protect your privacy. “Information security” refers to efforts to keep an attacker

from getting personal information against the wishes of both the consumer and the possessor of the information. A locked safe containing important documents is a form of information security. This paper does not address online privacy, forms of online crime not related to personal information (such as child pornography, discussed by Moore et al. 2009), or online security at a national level¹⁸. Readers interested in the online privacy should refer to Friedman (2009) for a brief overview or Lenard and Rubin (2010) for a more detailed discussion.

This paper reviews the work of economists in information security so far¹⁹. The first section summarizes the types of attacks, the technical mechanisms (as opposed to policy or incentive mechanisms) to fight them, and looks into the scope of the problem, as revealed by empirical investigations. This is followed by a brief aside regarding the technology used to protect information used in retail transactions. The third section discusses the theories of market failure that underlie information insecurity. The fourth section presents private solutions to the incentive problems, followed by policy solutions in the fifth section. Finally, I discuss implications for future technologies, particularly cloud computing.

2.2 The Problems: What Are They and How Big Are They?

There are four basic security problems faced by consumers, Internet Service Providers (ISPs), online retailers, security firms, and other stakeholders. Some of these

¹⁸ Eeten and Bauer (2009) argue that national cybersecurity is different in that it must try to prevent catastrophic harm, even when the probability of such harm is very small, and that the marginal thinking used in the economics of private information security is therefore not as relevant.

¹⁹ Previous literature reviews include Anderson and Moore (2006) and Moore et al. (2009).

problems are closely related, so these categories are somewhat arbitrary²⁰. House of Lords (2007) and Moore et al. (2009) provide good introductions to these basic security problems. They are:

Phishing: In its most basic form, phishing is accomplished by sending out spam emails to millions of people requesting that they visit a site (often a banking site) and login to verify some information. The site to which the user is directed is a front, intended to collect the user's information in order to commit identity theft. Banks stop phishing by hiring security firms to search out such fake sites and send removal requests to the businesses hosting them.

Malware: Viruses, trojans, spyware, and other malicious programs are classified as malware. Malware are primarily distributed via attachments in spam emails and using by exploiting vulnerabilities in web browsers. Once designed to wreak havoc on users computers or networks, often for bragging rights, malware is now primarily used for stealthily developing botnets. The software that protects against malware is usually referred to as antivirus software, although it usually protects against several forms of malware, rather than just viruses. More recently, Google and StopBadware (a nonprofit anti-malware organization) have coordinated their activities to stop sites hosting Malware (Day et al. 2009). Google search results indicate whether or not a site is on the StopBadware list of malware hosts, and Google's Chrome browser even displays a warning page before allowing users to

²⁰ For example, a botnet represents intrusions on thousands of computers, and is therefore an attack. It is also a *means* for an attack when used for, say, DDoS, or for dynamically hosting phishing sites.

access such a site. Malware is one of the few means that can be used to defeat encryption technologies used for sending personal information in online shopping (a keylogger, for example, could record the username and password of a shopper).

Botnets: A botnet is an army of bot (or “zombie”) computers. The person in charge of the botnet—the “botnet herder” or “botnet master” can gain access to the computers to make them do simple tasks. Because these tasks are simple, and modern computers are powerful and complicated, users never realize their machine has been co-opted. The computer can then be used to send out more spam email (collecting more bots for the botnet), dynamically host phishing sites, committing DDoS attacks (see below), or collecting personal information directly (in the case of spyware). A botnet can be rented from the botnet master by someone wishing to use it for these purposes; thus the motivation for building botnets is financial (Li et al., 2009). Again, the primary tool used against botnets is antivirus software, although network monitoring tools can also be used to find potentially infected computers. The CSI/FBI surveys (2002 to 2008) found antivirus software and firewalls were the primary technology defenses against attacks. The surveys do not make explicit which forms of attacks these technologies are intended to stop, but they should apply primarily to botnets and the following category.

DDoS: A Distributed Denial of Service attack is a barrage of simple requests, sent to a target server or group of servers. All the computers in the botnet

simultaneously attack these servers, overwhelming them with more messages than the servers can process, causing an internet traffic jam, or even crashing the server. If the server is hosting a website, the site will be unavailable, or if the target is an ISP, internet access may become unavailable to the ISP's customers. Stopping a DDoS in progress is difficult, because it comes from so many computers all at once. It is difficult to sort out real requests from fake ones. It is better to stop a DDoS before it happens by stopping the botnet from forming.

The scope of these problems is hard to estimate. Surveys are subject to reporting bias; firms suffering from weak security may be unwilling to disclose this, even anonymously, and security firms may exaggerate their success (Moore et al. 2009). This is discussed in more detail in the section on law enforcement solutions. Several organizations have nonetheless attempted to estimate the size of losses due to online security breaches.

Before we consider the losses, however, let us consider the size of the U.S. online economy. The Census Bureau (2009) estimates that total e-commerce in the U.S. was \$3.3 trillion in 2007, but this includes business-to-business shipments, sales, and revenue, so some of these are intermediate goods. Business-to-consumer shipments, sales, and revenue were \$251 billion in 2007, or around 1.7% of U.S. GDP.

The International Telecommunications Union (2008) estimates the costs of dealing with malware (which is calculated by adding the costs of dealing with malware-created problems to the deadweight loss represented by payments to malware authors and botnet masters) are at 0.2 to 0.4 percent of global GDP. The estimate is crude by their

own admission. The authors also suggest that all surveys probably underestimate the losses, because so many victims are reluctant to reveal that an event occurred. A 2005 FBI survey of IT professionals found that the costs to U.S. businesses of dealing with computer crime are at least \$67.2 billion per year.

The Ponemon Institute has conducted a series of annual studies (the 2006 through 2009 studies are easily accessible online). They investigate the cost to firms of data breaches of all kinds. The cost of a breach ranges from \$182 per consumer record (lost, stolen, or compromised) in 2006 to \$204 per consumer record in 2009. This is, on average, about the rate of inflation over this period, but some years experienced dramatic jumps, while others experienced insignificant increases, for reasons that are not apparent. The most recent survey found that the average cost to an organization of a data breach was \$6.75 million. Firms responding to the surveys described these costs as primarily resulting from “customer opportunity costs”—the costs of increased turnover of customers and increased difficulty of getting new customers. Breaches due to third parties (i.e., not the company or its customers) ranged from 30 to 44% of all breaches in every year except 2009, when breaches from malicious attacks and botnets doubled. Lost or stolen laptops, USB memory sticks, and other devices were either the most frequent or second most frequent cause of breach, depending on the year. Malicious breaches are as much as 40% more costly than breaches due to negligence (such as lost hardware).

The Computer Security Institute and FBI have jointly surveyed organizations regarding computer crime and security every year since 1996; the surveys from 2002 and later are easily obtained online. Each year they surveyed hundreds of organizations, and their samples consist of roughly equal numbers of for-profit and non-profit organizations

in various industries (although there is an “other” industry whose status I could not determine). The percentage of respondents reporting unauthorized breaches declined over the post-2001 period, going from 60% in the 2002 survey to 43% in 2008²¹ (with a small jump up in 2004 that was later reversed). Unlike the Ponemon Institute studies, viruses are found to be the primary source of security incidents, followed by insider abuse or theft/loss of mobile devices.

A large market for antivirus software has evolved opposite malware, in a nonstop arms race. The Gartner Research organization estimates that the worldwide market for security software had revenue of \$13.5 billion in 2008 (the fraction of this that includes “Endpoint Protection Platform” software—which is what Gartner calls software that protects individual users’ computers from malware, such as antivirus programs—is not available without purchasing the full report from Gartner).²²

Attacks meant to steal personal information ultimately may result in identity fraud. Javelin Strategy & Research have conducted a series of consumer surveys regarding identity fraud. In their 2008 study, they found that theft of personal information was overwhelmingly accomplished through traditional offline methods, with only 12% of identity theft occurring through online methods. They distinguish between identity theft—the act of stealing personal information—and identity fraud, which is the act of actually using personal information. In the 2010 survey most victims did not experience any out-of-pocket costs (presumably they notified their credit card company and/or bank in time), but among those who did suffer loss, the average out-of-pocket cost was \$373. The 2009 study shows an erratic pattern in average fraud amounts over time; there does

²¹ There seems to have been a slight change in the way the survey asked about breaches in the 2007 survey, but the results appear comparable.

²² <http://na2.www.gartner.com/it/page.jsp?id=1031712>, last accessed 4-20-10.

not seem to be a clear upward or downward trend from 2003 to 2008 (see their Figure 8; losses did fall substantially in 2006, but then rose in 2007 and 2008). These studies also provide explanations of the various kinds of identity fraud and theft techniques, as well as useful advice to consumers who wish to avoid or respond to identity theft and fraud.

The fact that these studies are measuring different things makes it difficult to get a clear impression of the scope of online security problems. Clearly the losses are “large” in absolute terms--\$67.2 billion and 0.2 to 0.4 percent of world GDP are big numbers, and a majority of organizations have experienced computer security breaches that with an average cost of several million dollars. It is also unclear whether this is an optimal level of security breaches—that is, should we spend more resources on fighting cybercrime, or have we reached the point at which the marginal cost equals the marginal benefit? The consensus in the literature seems to be that there are market failures (discussed in the section after the next one) that have workable private and public solutions, and we therefore are not doing enough to combat these online security problems.

2.3 An Aside: Retail Internet Security Technology

This paper mostly avoids the topic of online shopping security because it is either a mostly solved problem (in the case of how to send encrypted data) or a problem covered indirectly by the other sections (specifically, malware, which can be used to circumvent these security technologies). I could find no papers reporting that firms frequently dealt with security breaches in the form of data taken from encrypted data

streams. For more on the technology and economics of encryption and privacy (as well as other interesting issues) see Friedman (2009)²³. How does this security work?

When a consumer shops online, he or she sends personal information (name, address, credit card number) to the retailer, and the retailer sends information back to the consumer (price, shipping cost, date of delivery). SSL, or Secure Sockets Layer, is the primary method by which personal information is sent securely over the internet between users to retailers. A “socket” refers to an Application Programming Interface (API) which two computers use to communicate. A “layer” refers to a functional component of a program that provides services to the processes running on layers above it, and requests services from processes running below it. SSL has gone through several revisions (including Transport Layer Security, or TLS), but this paper does not deal with the technical details beyond a brief overview.

When a consumer wishes to send personal information such as a credit card number to a website the site directs the consumer to a secure page, as indicated by https:// (rather than http://). The site also sends the consumer a digital certificate, guaranteed by Verisign, Thawte, or one of many other SSL providers. This digital certificate can be checked against information stored in the consumer’s browser software (and which ships with modern browsers), allowing the user to verify the site’s credentials. The consumer can now use the site’s *public key* to encrypt information and send it to the site (the choice of “key” to describe this is perhaps unfortunate; “public lock” might be a better term)²⁴. The site (and no one else) possesses a *private key* which can be used to decrypt the

²³ Game theorists may be interested in related papers from the game theoretical literature on communication. For example, see Barany (1992).

²⁴ Encryption is basically accomplished by using an algorithm to scramble the information. The algorithm is easy to do, but hard to *undo*—unless one has the private key.

information. The information that the consumer initially sends is the *session key*, a key unique to this transaction, generated from a random number. Now the site and the consumer both have the session key, and they can use it to securely send information back and forth to each other (so long as there are no flaws in the programming for the process; such flaws can be exploited to get the session key). This explanation skips over some verification steps and simplifies the role of SSL certificate providers, but nonetheless accurately summarizes the process.²⁵

To a third party “listening” in to the stream of data between the computers, the data sounds like indecipherable noise. There are other ways that security could be compromised, however. Rather than trying to intercept communications, attackers try to breach corporate networks in order to remove personal information from databases. For example, on March 29, 2010 monoprice.com revealed that its servers were breached, resulting in the theft of customer names, credit card numbers, and other personal information.²⁶ In 2009 three hackers stole at least information for 130 million credit and debit cards from several companies using “SQL injection attacks”²⁷ Companies try to protect their data using encryption, but it is difficult to remove all vulnerabilities.²⁸

As mentioned in the first section, other avenues are also available to attackers. Viruses, worms, spyware, and other “malware” can all capture personal information by installing themselves on users’ computers, rather than attacking the retailers. The data can

²⁵ For a more detailed explanation of the process, see http://www.ourshop.com/resources/ssl_step1.html, last accessed 4-19-10.

²⁶ The letter to the New Hampshire Attorney General’s Office is available here: <http://doj.nh.gov/consumer/pdf/monoprice.pdf>, last accessed 4-29-10.

²⁷ http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect/, last accessed 4-29-10.

²⁸ For a large list of database breaches, see <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>, last accessed 4-29-10).

then be transmitted elsewhere (prior to its encryption) for a variety of uses, from simple identity theft to blackmail.

2.4 The Incentive Problems of Information Security

Economists have contributed little to the literature discussed this far, aside from helping to measure the costs of data breach. Economics becomes important to the information security literature when one considers the incentives which drive individuals and firms to respond to security threats, and whether or not those responses are optimal. There are two primary market failure arguments invoked in regards to the protection of personal information: Externalities (Anderson et al. 2009, Anderson and Moore 2006, Kesan et al 2005, Bohme and Kataria, House of Lords 2007) and the “Lemons” asymmetric information problem (Anderson et al. 2009, Day et al. 2009, Anderson and Moore 2006, Moore et al. 2009). They are discussed below, followed by a brief discussion of other possible economic arguments for inefficiently low investment in information security.

Externalities are everywhere in information security. Anderson and Moore (2006) argue that network security is of the “weakest link” type—a single poorly-secured computer can allow entry to a network, imposing costs on the other users and/or the parent organization. A user who does not keep antivirus software up-to-date is mostly imposing costs on others (because, as mentioned before, malware may merely be a means to creating a botnet to attack someone else). This applies not only to individual users, however. The externality argument also applies to ISPs, which may be reluctant to take security steps such as finding and removing bot computers on the network, particularly as

doing so requires making costly support calls, and the costs of malware fall mostly on other networks (Eeten and Bauer 2009). Software suppliers, too, may not find it worth their while to close security holes in their software if the costs are likely to fall on those who are not themselves or their customers. Websites may unknowingly distribute malware (through third party advertisements) or otherwise provide poor security, with little incentive to do anything about it (Day et al. 2009). Attacks that succeed against one firm might, through a network, allow access to other firm. Also, due to similarity of systems across firms, an attack that succeeds against one system may work against other firms with similar systems, even if they are not connected by a network (Ogut et al., 2005). Even actions as simple as failing to report breaches out of fear of bad publicity or giving an advantage to competitors (CSI/FBI 2002-2008) impose costs on others.

Kunreuther and Heal (2003) formalize the externality in a model of interdependent security. The focus of the paper is security in general, rather than information security specifically, but they do discuss what makes information security different. In particular, computer security has a significant public bad nature (as opposed to the mostly private bad nature of a bomb on an airplane). This causes firms or users to underinvest; even if they do their part to protect a network, the failure of someone else within the network to protect their computer could end up harming everyone inside the network. Ogut et al. (2005) develop a model of interdependent risk of security breach across firms, and conclude that this interdependent risk leads to underinvestment (although their model is focused on the effects of cyberinsurance, which is discussed in the “private solutions” section of this paper).

These are powerful arguments for why we should expect nearly everyone online to underinvest in security. It is worth pointing out, however, that the existence of an externality does not necessarily mean that the unregulated market outcome is inefficient. In the case of an *inframarginal* externality, the marginal externality goes to zero before the equilibrium is even reached. If, for example, education produces positive externalities through five years of schooling, but everyone chooses to achieve at least ten years of schooling, the externality is irrelevant and the unregulated market outcome is efficient. This could be true in the case of businesses protecting customer records (or other confidential information) from external attack. While it is true that costs will also fall on customers whose records are stolen, if the damage to the firm is large enough (in terms of recovery costs, legal fees and damages, and the costs of customer turnover), it will have sufficient incentive to take efficient precautions.

Do firms face substantial costs as a result of breach? Campbell et al. (2003) conducted an event study for security breaches and found that breaches produced significant negative abnormal returns when the breaches involved confidential information, but were not significant when confidential information was not stolen (as in the case of denial of service attacks). Acquisti, Friedman, and Telang (2006) also conducted an event study and found that a reported information security breach created abnormal negative returns of slightly more than half a percent, but this only lasts three days. Cavusoglu et al. (2004) found that firms lost 2.1% of their value in the two days after disclosure of a breach, in yet another event study. Telang and Wattal (2007) find that disclosure of a vulnerability within a software product correlates with a loss of 0.6% of a firm's stock price, and that the share lost is larger in a more competitive market or if

the firm is small. Davis et al. (2008) look at traffic of sites that have experienced a security incident, but find no effect. Customers do not seem to take their business elsewhere. Taken together these papers provide a murky picture of whether the market sufficiently punishes firms for failing to take precautions—there is a loss of market value, but it may be short-lived, and a site’s traffic does not fall after a breach. See the “The Problems: What Are They and How Big Are They” section above for estimates of the costs to firms of information security breaches.

The second basic incentive problem pointed out by economists is the Lemons asymmetric information problem made famous by Akerlof (1970). As applied to information security, the problem is that consumers of security find it difficult to compare the effectiveness of security companies and software (Anderson et al. 2009, Day et al. 2009, Anderson and Moore 2006, Moore et al. 2009). Providing better security is surely more costly than providing worse security, so providers with poor quality charge lower prices. Those shopping for security, being unable to make meaningful comparisons, buy the cheaper products, and poor quality drives out high quality. A consumer buying antivirus software has no clear metrics with which to compare programs. Web hosts may suffer from a similar problem: those who would hire them to host their websites cannot tell which web hosts are more secure, so hosts tend to provide bad security (Day et al. 2009).²⁹

Other researchers have suggested additional causes of poor information security. Bradford et al. (2009) found that nonbanks play many roles in processing payments, more

²⁹ My personal experience with computer geeks suggests that this effect may be exaggerated, at least for antivirus software. There seem to be clear favorites among these groups. These favorites change over time, and they are not necessarily well known names; Eset’s NOD32 is well thought of by many techies. These are only a fraction of all users, however, so the asymmetric information problem may still be serious.

so in the U.S. than in Europe. This may allow more opportunities for attacks, as information changes hands more often, and there are more points of access to data. The damage can be high because of concentration in these industries due to economics of scale (that is, a single firm may have vast quantities of data).

Anderson et al. (2009) suggest that law enforcement is too slow and fragmented across agencies. The CSI/FBI surveys show that many organizations do not report breaches to law enforcement because of simple lack of awareness that it is an option.

Beautement et al. (2009) look at the usage of USB sticks, and find that there is a tradeoff between data availability and confidentiality; USB sticks make it easy to carry data around, but they are also easy to lose. Their model, calibrated on survey results, supports the hypothesis. They find that individuals often carry USB sticks even when it is against IT policy, although they also find that more IT support correlates with a higher probability of using encryption to protect data on USB sticks.

Managers may make mistakes when deciding how much to invest in information security due to confusion over the meaning of security metrics, according to Hulthén (2009). In particular, Return on Security Investment may not mean what managers think it means. The authors suggest transformation of security terms (vulnerability, breach loss, threat, etc.) into Value-at Risk measures.

Anderson et al. (2009) and House of Lords (2007) suggest that firms use licenses to disclaim responsibility for security failures, imposing the costs of breach on others. They do not consider the possibility that this is efficient. Suppose that these firms are not the low-cost avoiders of security failure. In that case, it is efficient for them to push the costs onto parties who can improve security at a lower cost. If, on the other hand, these

firms *are* the low-cost avoiders of security failure, then they could profit by improving security and charging a higher price.

Moore et al. (2009) argue that phishing sites stay up longer than they need to as a result of poor information sharing among firms that specialize in locating and taking down such sites—they have not learned the lesson that the antivirus industry learned in the previous decade.

Anderson et al. (2009) suggests that lack of diversity in platforms (including operating systems such as Windows) makes attacks easier and more damaging. In a June 3, 2010 article in the online magazine Slate, Farheed Manjoo aptly expresses the conventional wisdom on this subject:

Windows is the main target of thieves who are trying to steal banking passwords; if you're on any other system, their malware simply won't run. Indeed, this is true for most malicious software... We rarely hear about malware infecting the Mac, but that's mainly because only around 5 percent of computers in the world are running the Mac OS. Hackers attack Windows for the same reason that robbers target banks—that's where the money is.

What can be done to improve information security? The next two sections discuss proposed solutions, private and public.

2.5 Improving Security: Private Solutions

One of the most prominent proposed solutions seems to have first been mentioned in the literature by Varian (2004): cyberinsurance³⁰. A firm that buys cyberinsurance is covered against losses incurred as a result of a data breach. Varian argued that efficient security effort could be elicited from individuals if insurers set an appropriate liability rule which only allows compensation to be paid when the insured takes the appropriate level of care. If the level of care is observable, this would avoid the moral hazard problem. Several writers have since worked on the subject in an effort to determine the effects of cyberinsurance on information security. In 2004 the CSI/FBI surveys began asking respondents about cyberinsurance. Only one-fourth to one-fifth of surveyed organizations had cyberinsurance. Many of the organizations surveyed (governments, for example) may not be prime candidates for cyberinsurance. Unfortunately the studies do not tell us the proportion of for-profit organizations that have cyberinsurance.

Bolot and Lelarge (2009) argue that cyberinsurance provides incentives to increased security if insurers can discriminate—that is, if they can charge higher premiums to policy holders with weaker security. Oguet et al. (2005) develop a model of cyberinsurance in this setting, and find that that interdependence of risks across firms leads firms to underinvest in security *and* insurance. The argument for underinvestment in security has been made in the previous discussion of externalities. The underinvestment in insurance occurs because insurers face larger, less controlled risks when interdependence is high, so they charge higher premiums, resulting in less cyberinsurance purchased by firms. As the insurance market matures, it is possible that cyberinsurance adoption will improve *if* insurers are better able to assess risk and the price of insurance falls. The price of insurance need not fall, however; it is also possible

³⁰ This is variously written as one word, two words, or hyphenated. I have opted for the simplest version.

for firms to substitute insurance for investment in security, which leads to higher risks for insurers, and therefore higher premiums.

Kesan, Majuca, and Yurcik (2005) look at actual implementation of cyberinsurance and find that, although it faces some obstacles, it could become an effective solution to security problems. They find that there are a variety of cyberinsurance products now available which pay firms in the event of data destruction, interruption of internet business, DDoS attacks, extortion, and fraud. Insurers provide assistance with security, including monitoring and risk assessment. Insurance agreements include measures to reduce moral hazard problems, including due care requirements (for example, the level of security cannot be allowed to drop below the level that existed during the initial assessment, and firms that do not back up data will not be compensated). Other measures include rewards for information leading to conviction of the cybercriminal and requirements to notify police.

Some problems still exist. The market is new and not yet standardized, so signing up is costly and time-consuming. So far only large firms can afford to insure their security. To put it another way, it is too costly to observe the precaution levels of smaller firms, so the moral hazard problem prevails, and the market for small-firm cyberinsurance does not exist. This problem might be reduced as the market for cyberinsurance matures and becomes standardized. Cyberinsurance might actually reduce externality problems by creating clear standards that firms—even those that are not insured—can follow. On the other hand, perhaps clear standards create a uniform defense that attackers can more easily circumvent.

Bohme and Kataria (2006) conclude that cyberinsurance works best when externalities within the firm are serious—when a security problem with one computer is likely to affect other systems inside the network. If, on the other hand, “internal correlation” (as they call it) is low, firms can self-insure and do not demand cyber-risk transfer. But it must also be the case that systems outside the network do not impose much risk, because insurers cannot pool risk across enough firms to cover this—they would have to charge high loads.

Another possible solution to the various online risks is to diversify the set of operating systems used. The rise of alternatives to Windows may reduce security problems for two reasons (As argued by Manjoo, 2010). First, if Windows is an inherently insecure platform, alternatives such as OS X, iPhone OS, Android, and Chrome OS may reduce security incidents. Second, Windows is also an attractive target for malware creators because it provides a large number of victims. The splintering of users into many different targets might make each less attractive. Building a botnet the size of one that was available with Windows might require writing malware that runs on several different kinds of devices, raising the costs of doing so. As supporting evidence, consider that the Financial Times reported on May 31, 2010 that Google plans to phase out internal use of Windows for security reasons. If there are economies of scale in writing malware that targets a particular operating system, having the market divided into many smaller operating systems might make malware less profitable to write. This cuts both ways; writing software to fight malware may also cease to enjoy economies of scale.

Security certification is another possible private solution. A firm can go through a certification process, during which its security procedures are inspected³¹. Firms that pass can display a certification seal on their website or in advertising, thereby notifying customers of their security status. Anderson and Moore (2006) point out that this, too, suffers from a lemons problem: consumers may find it difficult to tell which seals are meaningful and which ones are not, resulting in only worthless certification. Edelman (2006) finds that sites with TRUSTe certification are *less* trustworthy than non-TRUSTe sites. This finding does not seem to apply to BBBOnline certification, but BBBOnline certification suffers from a long backlog in applications. There are other ways to notify customers of security on a site. Miyazaki and Fernandez (2000) examined privacy and security statements at 381 retail sites in the U.S. Half had statements describing how they kept transactions secure. Less than 6% had a credit card fraud guarantee. These numbers varied for different types of goods. For example, 92.3% of computer hardware sites had secure transaction statements, but only 11.8% of rug and carpet sites had such statements.

Moore et al. (2009) point out that antivirus developers have improved quality by agreeing to share information with each other when new viruses are found, and they suggest that anti-phishing organizations could benefit from the same kind of information sharing. Eeten and Bauer (2009) describe how ISPs rely on reciprocity and information sharing to remove bots or dangerous sites from each other's networks. An ISP that is found to have bots on its network might be asked by a victim (or potential victim) to remove them. Failure to do so could mean that the complaining firm refuses to help the offending firm in the future, and could even get the offending firm added to a black list. The customers of a blacklisted ISP would find themselves unable to send or receive

³¹ Or its privacy procedures, or customer service, or whatever is being certified.

traffic from some other ISPs, which is sure to impose costs on the offending ISP in the form of support calls. Information sharing and reciprocity can overcome some information security externalities.

Contracts and common law duties may bind firms to protect personal information and give them an incentive to do so, if blame can be clearly assigned.

2.6 Improving Security: Policy Solutions

Governments have also devoted some attention to information security, and researchers have suggested additional policies to improve security. The Gramm-Leach-Bliley Act of 1999 (also known as the Financial Services Modernization Act of 1999) requires all financial institutions to have a plan for the security of personal information. The act lays out specific measures which must be taken (such as having at least one employee whose duty is to manage security). Additional regulations were passed in 2001 as part of Section 501 of the Gramm-Leach Bliley act, giving various agencies (The Fed, the Office of the Comptroller of the Currency, the FDIC, and the Office of Thrift Supervision) the mandate of enacting additional regulations regarding data security of financial institutions. HIPAA's 2003 security regulations imposed the GLB security requirements on health care providers. See Keitel (2008) for further discussion of policy responses to information security problems.

While looking for preexisting regulations regarding information security I came across several sites which suggested that the Sarbanes-Oxley Act (which was intended to improve the accuracy of corporate financial information) is expected to increase corporate information security. I cannot find anything in the bill directly addressing this.

Information security might be useful in reducing fraud, which would improve financial reports, but Sarbanes-Oxley does not mandate this. The CSI/FBI surveys began asking about Sarbanes-Oxley Act in 2004, and found that more than half the organizations surveyed in the financial, utility, and telecom sectors reported increased interest in information security as a result of Sarbanes-Oxley, but less than half (in some cases, far less) of those in other sectors reported increased interest as a result of Sarbanes-Oxley.

House of Lords (2007) points out that there are no federal data breach laws in the U.S. (which would, for example, require disclosure by entities, banks or otherwise, that suffer theft of personal information due to a breach). At the time of that writing, however, there were 35 states with laws regarding data breach, some of which impose “tough penalties”, and require notification of authorities and/or individuals whose data has been stolen³². The U.K. does not have a data breach law.

Anderson et al. (2009) were asked write a list of policy recommendations for the European Network and Information Security Agency (ENISA), and contains the most comprehensive list of policy proposals. House of Lords (2007) also contains several policy recommendations. The following is a discussion of the policies they and others have suggested.

Anderson et al. (2009) and House of Lords (2007) recommend security breach notification requirements (notifying law enforcement, the press, and affected consumers) and laws that mandate disclosure of losses to electronic crime (for the sake of investors and for policymakers to better understand the scope of the problem. The Ponemon Institute (2010), however, found that a rapid response to breach may actually drive costs

³² For a somewhat outdated list of state breach laws, see “State PIRGH Summary of State Security Freeze and Security Breach Notification Laws” (2006), available online at <http://www.pirg.org/consumer/credit/statelaws.htm>, last accessed 6-3-10.

up. Organizations that notified victims within a month of breach had 12% higher costs than those that did not. Yet the causation could go the other way—perhaps firms with higher costs had more serious problems, and felt compelled to notify faster. The authors did not attempt to determine direction of causation.

Lenard and Rubin (2006) examine the economics of breach notification laws in detail. They argue that the costs of a breach fall almost entirely on firms that store information, and that, as a result, investment in security should be only slightly suboptimal (again, as I have argued above, if the externalities are inframarginal, private investment in security may be optimal). There may nonetheless be insufficient incentives for firms to provide notice to victims of identity theft resulting from security breaches, due to the many entities involved with processing payments and storing and transmitting data. The benefit of notification is that affected consumers may be able to take steps to reduce the damage caused by identity theft, and they estimate that the expected benefit to an average consumer is \$10 or less. The costs of providing notification include direct costs, such as reconstructing the data to determine whose data was stolen and actually notifying them, and indirect costs, such as the possibility that consumers retreat to real-world transactions, which are actually less secure. These costs are difficult to estimate, but Lenard and Rubin suggest that it is unlikely that notification would pass a benefit-cost test. They therefore caution against laws requiring disclosure. They further suggest security policies at firms are driven by the state with the most stringent security and notification laws, due to the non-geographical nature of internet transactions. Firms do not want to tailor their security levels in each state to that state's laws; keeping up with changes in the law are too costly. Rather, they find the state with the most stringent (and

costly) laws and follow those. Therefore it may make more sense to have national security and notification laws, rather than using a federalist approach.

There is little evidence available on the effects of breach disclosure laws. Romanosky et al. (2008) look at state-level variation in breach disclosure laws and reported breaches using a panel of data from 2002 to 2007. They find that breach disclosure laws have a small effect on the rate of identity theft—a slightly less than 2% decrease. They also estimate that the savings to consumers of this reduction in identity theft would have been around \$1 billion in 2005.

Anderson et al (2009) also suggest that governments mandate all equipment and software be sold secure (up-to-date with automatic patching enabled) by default. Requiring that software be sold up-to-date is a strange suggestion for retail software sold at brick-and-mortar stores; it must sit on shelves, and will therefore become out of date. This policy recommendation would be more relevant for digital distribution, but it is not clear to me that out-of-date software is a problem there. The authors also suggest that patches to security software should be free.³³

There is a debate over whether firms should be required to disclose vulnerabilities as soon as they are discovered. Although Anderson et al. (2009) supports this, Rescorla (2005) finds that if the number of vulnerabilities in software do not decrease over time, disclosure of vulnerabilities does not improve security. Disclosure, he argues, only makes sense if vulnerabilities would otherwise be discovered by those who intend to break through security. Ozement and Schechter (2006) found that in the case of the FreeBSD operating system, the number of vulnerabilities discovered has declined. Ozment (2005)

³³ They do not elaborate on what this might mean. Many software patches are already free, and the ones that are not are labeled “upgrades” or as entirely new versions. It might be difficult to define a patch.

found that vulnerabilities in an operating system are likely to be discovered. These findings support mandatory rapid vulnerability disclosures. Arora et al. (2008) develop a theoretical model to examine incentives to disclose vulnerabilities, and find that in the presence of negative externalities from breach, software vendors have an incentive to release security patches more slowly than is socially optimal. A social planner could encourage quicker patching by shrinking the window during which the developer is allowed to work on a patch without disclosing the existence of the vulnerability (the social planner will announce the vulnerability at the end of the window). They also find that the quality of the security patch does not necessarily increase if the software vendor is given more time. Day et al. (2009) suggests that the disclosure debate may be irrelevant for hosted malware (that is, malware hidden in the code on a web page and installed unbeknownst to the web surfer), as existing efforts are effective. If Google's search results show a site hosts malware, giving them a grace period to correct it (prior to warning the public) increases the number of infections, decreases the incentive to fix the problem quickly, *and* decreases the incentive to stop such problems before they occur. Google's and StopBadware's efforts compel firms to internalize the malware-caused externality.

Several authors recommend assigning liability to firms that suffer breach (Anderson et al. 2009, House of Lords 2007, Varian 2004, Ogut et al. 2005). The goal of assigning this liability is to force firms to internalize the security externality. In House of Lords (2007) one interviewee suggested that this could result in more closed systems, as vendors prohibit third party software for fear of interaction with their own software causing security weaknesses. Establishing who is liable for what can also be an issue; if a

virus attacks a vulnerability in my Windows PC, is that Microsoft's fault or the fault of my antivirus provider?

Moore et al. (2009) and Anderson et al. (2006) call for more global law enforcement cooperation, in the form international or EU task forces. Law enforcement efforts are currently slow and fragmented across agencies and countries. Given the international scope of the internet, coordination is necessary to find and stop attackers. House of Lords (2007) calls for similar international cooperation and the creation of a centralized reporting system for breaches, combined with mandatory disclosure of breach. The externality argument applied to private security efforts also applies to public efforts, however. Steps will have to be taken to ensure that these cybercrime police do not simply pass the buck onto their counterparts with whom they are supposed to be cooperating. The 2008 CSI/FBI survey respondents listed "Believed Law Enforcement Couldn't Help" as their second most important reason for not reporting breaches of security (behind "Incidents Too Small to Bother Reporting"). Overcoming this skepticism will be difficult.

"Virtual machine honeypots" are a novel solution investigated by Li et al. (2009). They suggest that networks of simulated computers be opened to infection; the botnet master then "infects" them and believes they are part of his network. They are really being monitored and controlled by anti-malware organizations. When the botnet master attempts to execute an attack, the virtual machines do not participate and the attack fails (or is significantly less successful than anticipated). The increased uncertainty regarding the success of an attack reduces the expected payoffs to parties who would rent botnets, thereby reducing the demand for the services of the botnet master, reducing the incentive

to create botnets. The proposal may have problems. For example, not all botnets are equally sophisticated; some may be able to figure out which machines are virtual. The authors are also vague on an important detail: Who will create and monitor these virtual machines? They are providing a public good, and may therefore be underprovided by the private sector. It is not clear if virtual machine honeypots are intended to be a public or private response to botnets. There may be some private stakeholders who are sufficiently large to have an interest in promoting internet-wide security—Microsoft, for example, has released a free antivirus program. Microsoft, Cisco, Google, and other large stakeholders may find virtual machine honeypots to be another useful tool for fighting malware and DDoS attacks.

Other solutions suggested by Anderson et al. (2009) include harmonizing dispute resolution procedures across the E.U. (between customers and payment service providers), legal sanctions against abusive online marketers, and more research on cybercrime.

2.7 Implications for the Future

As computers grow in power and high-speed internet connections become ubiquitous (and even wireless), we should expect botnets to grow larger. The increase in computer speed may make new defenses against them possible, and increased diversity of operating systems may help as well. Some newer operating systems use “sandboxing” to keep third party applications from affecting the rest of the machine. The applications run inside a restricted space, unable to access all the device’s features.

The availability of high speed internet connections has also led to “cloud computing”, or the hosting of important applications and data outside of local client computers. For example, one can now use Google Docs to create and edit word processor documents, spreadsheets, and presentations using only a web browser. The user need not install an office suite on his or her PC, and the documents are hosted online rather than stored locally. This provides one the ability to edit one’s documents on any computer with an internet connection, with little worry about backing up the data. Cloud computing has been around for some time in the form of web mail (Gmail, Yahoo mail, Hotmail, etc.), but the development of other online applications is relatively new.³⁴ Microsoft is working on its own cloud version of its Office software as well, and provides tools (known as Azure) for developing other cloud applications. There is even a cloud gaming service in development, called Onlive, which streams video games to players in real time.

What are the implications of cloud computing for information security? Like webmail, the hosting of files online enables low-cost scanning by the host for malware. Google can scan attachments in gmail and notify the user if they are infected. Similarly, Google Docs could provide a means of protection against malware; it might be difficult to put harmful code into documents created online. Therefore we might expect cloud computing to usher in an age of safer computing, at least for information that need not be stored or worked on locally.

On the other hand, if a breach does occur in the cloud, it might create much larger losses than breaches in the past. Suppose, for example, that someone found a way to successfully attack Google Docs. The attacker could access the stored documents (up to)

³⁴ Writely, which forms the basis of the Google Docs word processor, was launched in 2005 by Upstartle. Google acquired Upstartle in 2006, and launched Google Docs in 2007.

millions of people. An attacker who penetrated Gmail, as was apparently accomplished from China in December 2009³⁵, could get personal information from millions of users, including their account information. In the most recent case only two gmail accounts were successfully accessed, and only in a limited fashion, but future breaches could be much more costly.

2.8 Conclusions

Information security is a difficult field because it pulls together research from very different areas—cryptography, economics, insurance, networking, etc.—and they must all work with data that is often incomplete, or worse, biased. There have nonetheless emerged some consensus views and policy recommendations.

In particular, researchers in the area act on the assumption that there is currently not enough information security, and this weak security is due primarily to negative externalities and an inability to judge the quality of competing security measures. Future research should focus on improving the quality of data available and determining the success or failure of different security measures. Experiments could be conducted with virtual machine honeypots, vulnerability markets, and other solutions. Developers may be able to further reduce security problems by considering incentive design at the very earliest stages of software and system development.

³⁵ See the Google Blog for details, <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>, last accessed 6-15-10.

References

- Acquisti, A., A. Friedman, and R. Telang (2006). "Is There a Cost to Privacy Breaches? An Event Study". Paper presented at the Twenty Seventh International Conference on Information Systems, Milwaukee 2006.
- Akerlof, G. (1970). "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics*, 84 (3): 488-500.
- Anderson, R. and T. Moore (2006). "The Economics of Information Security," *Science*, 314, 610-613.
- Anderson, R., R. Boehme, R. Clayton, and T. Moore (2009). "Security Economics and European Policy". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Arora, A., T. Rahul, X. Hao (2008). "Optimal Policy for Software Vulnerability Disclosure," *Management Science*, 54 (4), 642-656.
- Bárány, I. (1992). "Fair Distribution Protocols or How the Players Replace Fortune," *Mathematics of Operation Research*, 17(2): 327-340.
- Beautement, A., R. Coles, J. Griffin, C. Ioannidis, B. Monahan, D. Pym, A. Sasse, and M. Wonham (2009). "Modeling the Human and Technological Costs and Benefits of USB Memory Stick Security". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Bradford, T., F. Hayashi, C. Hung, S. Weiner, Z. Wang, R. Sullivan, and S. Rosati (2009). "Nonbanks and Risk in Retail Environments". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.

- Campbell, K., L. Gordeon, M. Loeb, and L Zhou (2003). "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, 11 (3) 431-448.
- Cavusoglu, H., B. Mishra, and S. Raghunathan (2004). "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce*, 9 (1) 69-104.
- Computer Security Institute (2002). "2002 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends*, 8 (1), 1-22. Available at <http://diogenesllc.com/2002cybercrimesurvey.pdf>, last accessed 6-8-2010.
- Computer Security Institute (2003). "2003 CSI/FBI Computer Crime and Security Survey," Available at <http://gamejam.cti.depaul.edu/~rburke/courses/f03/ect582/docs/FBI2003.pdf>, last accessed 6-8-2010.
- Computer Security Institute (2004). "2004 CSI/FBI Computer Crime and Security Survey," Available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf, last accessed 6-8-2010.
- Computer Security Institute (2005). "2005 CSI/FBI Computer Crime and Security Survey," Available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf, last accessed 6-8-2010.
- Computer Security Institute (2006). "2006 CSI/FBI Computer Crime and Security Survey," Available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf, last accessed 6-8-2010.

- Computer Security Institute (2007). "2007 CSI/FBI Computer Crime and Security Survey," Available at <http://www.sis.pitt.edu/~jjoshi/courses/IS2150/Fall09/CSIFBI2007.pdf>, last accessed 6-8-2010.
- Computer Security Institute (2008). "2008 CSI/FBI Computer Crime and Security Survey," Available at <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>, last accessed 6-8-2010.
- Davis, G., A. Garcia, and W. Zhang (2009). "Empirical Analysis of the Effects of Cyber Security Incidents," *Risk Analysis*, 29 (9), 1304-1316.
- Day, O., R. Greenstadt, and B. Palmén (2009). "Reinterpreting the Disclosure Debate for Web Infections". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Edelman, B. (2006). "Adverse Selection in Online 'Trust' Certifications", Working Paper, available online at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.9855&rep=rep1&type=pdf>, Last accessed 6-10-10.
- Eeten, M., and J. Bauer (2009). "Emerging Threats to Internet Security: Incentives, Externalities, and Policy Implications". *Journal of Contingencies and Crisis Management*. 17 (4), 221-232.
- FBI (2005). *2005 FBI Computer Crime Survey*. <http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf>, last accessed June 2, 2010.
- Friedman, D. (2009) *Future Imperfect*. New York: Cambridge University Press.

- Gelles, D., and R. Waters (2010). "Google Ditches Windows On Security Concerns," *Financial Times*, May 31, 2010. <http://www.ft.com/cms/s/2/d2f3f04e-6ccf-11df-91c8-00144feab49a.html>, last accessed June 3, 2010.
- House of Lords (2007). "Personal Internet Security," 5th Report of Session 2006-2007.
- Hulthén, R. (2009). "Communicating the Economic Value of Security Investments". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- International Telecommunications Union (2008). *ITU Study on the Financial Aspects of Network Security: Malware and Spam*. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf>, last accessed June 4, 2010.
- Javelin Strategy & Research (2008) "2008 Identity Fraud Survey Report: Consumer Version".
- Javelin Strategy & Research (2009) "2009 Identity Fraud Survey Report: Consumer Version".
- Javelin Strategy & Research (2010) "2010 Identity Fraud Survey Report: Consumer Version".
- Jean, B., and M. Lelarge (2009). "Cyber Insurance as an Incentive for IT Security". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Keitel, P. (2008). "Legislative Responses to Data Breaches and Information Security Failures". Payment Cards Center Discussion Paper No. 08-09.

- Kesan, J., R. Majuca, and W. Yurcik (2005). "Cyberinsurance as a Market-Based Solution to the Problem of Cybersecurity: A Case Study," *The Fourth Workshop on the Economics of Information Security*.
- Kunreuther, H. and G. Heal (2003). "Interdependent Security". *Journal of Risk and Uncertainty*, 26 (2), 231-249.
- Lenard, T., and P. Rubin (2006). "Much Ado About Notification," *Regulation*, 29 (1), 44-50.
- Lenard, T., and P. Rubin (2010). "In Defense of Data: Information and the Costs of Privacy," *Policy & Internet*, 2 (1), 149-183.
- Li, Z., Q. Liao, and A. Striegel, (2009). "Botnet Economics: Uncertainty Matters". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Manjoo, F. (2010). "The End of Malware? How Android, Chrome, and the iPad are shielding us from dastardly programs". *Slate*, June 3, 2010.
<http://www.slate.com/id/2255917/>, last accessed June 3, 2010.
- Matsuura, K. (2009). "Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Miyazaki, A. and A. Fernandez (2000). "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing*. 19 (1), 54-61.
- Moore, T., R. Clayton, and R. Anderson (2009). "The Economics of Online Crime," *Journal of Economic Perspectives*, 23 (3), 3-20.

Moore, T., and R. Clayton (2009). "The Impact of Incentives on Notice and Take-down".

In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*.

Springer.

National Cyber Security Alliance (2005). *AOL/National Cyber Security Alliance (NCSA)*

Online Safety Study,

<http://staysafeonline.mediaroom.com/index.php?s=43&item=26>, last accessed

May 31, 2010.

National Cyber Security Alliance (2008). *2008 NCSA/Symantec Home User Study*,

<http://staysafeonline.mediaroom.com/file.php/100/2008+NCSASymantecStudyA>

[analysis.pdf](#), last accessed May 31, 2010.

Ogut, H., N. Menon, and S. Raghunathan (2005). "Cyber Insurance and IT Security

Investment: Impact of Interdependent Risk," 4th Workshop on the Economics of Economics Security.

Ozment, A. (2005). "The Likelihood of Vulnerability Rediscovery and the Social Utility

of Vulnerability Hunting." Presented at the Fourth Workshop on the Economics of Information Security, June 2-3, 2005.

Ozment, A. and S. Schechter (2006). "Bootstrapping the Adoption of Internet Security

Protocols." Presented at the Fifth Workshop on the Economics of Information Security, June 26-28 2006.

Ponemon Institute (2006). *2006 Annual Study: Cost of a Data Breach*.

Ponemon Institute (2007). *2007 Annual Study: U.S. cost of a Data Breach*.

Ponemon Institute (2009). *Fourth Annual U.S. Cost of Data Breach Study*.

Ponemon Institute (2010). *2009 Annual Study: Cost of a Data Breach*.

- Rescorla, E. (2005). "Is Finding Security Holes a Good Idea?" *IEEE Security and Privacy*, 3 (1), 14-19.
- Romanosky, S., R. Telang, and A. Acquisti (2008) "Do Data Breach Disclosure Laws Reduce Identity Theft?" SSRN Working Paper No. 1268926.
- Schneier, B. (2000) *Secrets & Lies*. Wiley.
- Sowa, S., L. Tsinas, and R. Gabriel (2009). "BORIS – Business-Oriented Management of Information Security". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Telang, R., and S. Wattal (2007). "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price," *IEEE Transactions on Software Engineering*, 33 (8) 544-557.
- U.S. Census Bureau, *E-Stats*. Available at <http://www.census.gov/econ/estats/2007/2007reportfinal.pdf>, last accessed 6-3-2010
- Varian, H. (2004). "System Reliability and Free Riding," Working Paper.
- Zhao, X., and M. Johnson (2009). "The Value of Escalation and Incentives in Managing Information Access". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.
- Zhuge, J., T. Holz, C. Song, J. Guo, X. Han, and W. Zou (2009). "Studying Malicious Websites and the Underground Economy on the Chinese Web". In: Johnson, M. (Ed.), *Managing Information Risk and Economics of Security*. Springer.

Chapter 3

Do Certification Seals Permit a Price Premium?

Mike Hammock

Abstract:

If some consumers care more about online privacy and security than others, and if providing privacy and security imposes opportunity costs on firms, then firms with more privacy and security measures should charge higher prices, and consumers who value these measures should be willing to pay higher prices. To test this, data on the prices and certification seals of websites was collected. Examination of the data reveals moderate evidence that firms with security seals enjoy a price premium, and weak evidence that sites displaying other seals enjoy a price premium.

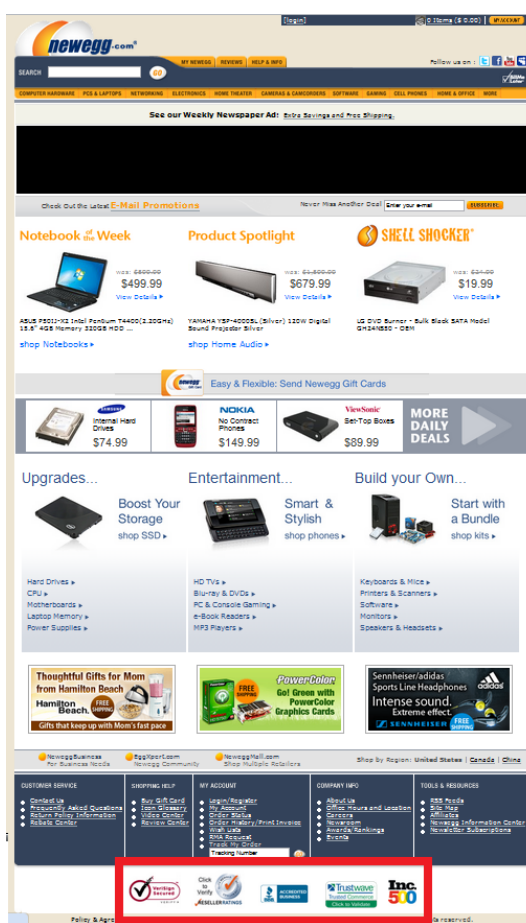
3.1 Introduction:

Internet security and privacy are of concern to economists because lack thereof may create deadweight losses. If consumers are unwilling to make purchases because of concerns about third parties obtaining their personal information, then value increasing exchanges are foregone. If websites are unable to provide assurances to customers that their personal information is safe, the result may be a kind of market failure.

Privacy and security are not the same thing, although they are related. A website provides *privacy* when it promises not to reveal the personal information of consumers to third parties. For example, a site might promise not to sell a user's email address and purchase history. Exceptions might be listed for some situations, such as requests made

by governments. *Security*, by contrast, prevents third parties from obtaining information against the will of the site and the consumer. SSL (Secure Sockets Layer) encryption is a common method of providing security for e-commerce sites. Certification seals, such as Verisign, Truste, and Scanalert, tell consumers that a site provides certain protections, and that a third party has vouched for those protections.

The seals are usually placed on the side or bottom of the site. Here, for example, is newegg.com's front page.





The seals have been highlighted by a red rectangle, added for clarity (not on the original site). Viewed more closely, these seals look like this:



Each is a clickable link which takes one to the certifying website. For example, clicking on the Verisign seal results in the following:

4/24/2010 22:57
secure.newegg.com uses VeriSign services as follows:

SITE NAME:	secure.newegg.com
SSL CERTIFICATE STATUS:	Valid (09-Apr-2010 to 21-Jun-2012)
COMPANY / ORGANIZATION:	NEWEGG INC City of Industry California, US

 Encrypted Data Transmission	This Web site can secure your private information using a VeriSign SSL Certificate. Information exchanged with any address beginning with https is encrypted using SSL before transmission.
 Identity Verified	NEWEGG INC has been verified as the owner or operator of the Web site located at secure.newegg.com. Official records confirm NEWEGG INC as a valid business.

For your best security while visiting sites, always make sure the address of the visited site matches the address you are expecting to see. Make sure that the URL of this page begins with "https://sealinfo.verisign.com" [>> REPORT SEAL MISUSE](#)

This allows the consumer to verify that the site provides the security promised by the seal.

In the current debate over online privacy and security it is assumed that consumers desire more of both. It is not clear that this is the case. Aside from privacy and security measures provided by websites, consumers may be protected by their banks, credit card agreements, identity-theft insurance, or other measures. Providing additional protection is presumably costly to websites or else they would provide the maximum

amount of security and privacy in all cases. Costs to websites include obvious expenditures, such as:

- Fees paid to seal providers for the right to display certification seals. These vary from seal to seal. The most basic Verisign SSL certificate (which provides a seal) is \$995 per year. The cost of BBBOnline's seal depends on the size of the company, and could range from hundreds to thousands of dollars per year.
- Fees paid to lawyers who help write a privacy policy or deal with breaches of privacy and security which occur

There are also less obvious expenditures, including:

- The costs of compliance with the requirements of a certification seal—for example, training employees, reorganizing a site, dealing with customer complaints in a more timely fashion.
- The opportunity costs of foregone sales of information.

If privacy and security are costly to provide, and if consumers are already satisfied with the level of protection websites provide, they should not be expected to be willing to pay higher prices for additional protection. If consumers *do* value privacy and security more than the cost of providing them, then we should observe a price premium at sites that provide additional protection. Certification seals could also raise prices by acting as a barrier to entry.

This paper extends the literature on prices and certification seals by considering a wide array of seals on a variety of products from many sites. The paper is divided into

five sections. First I review the economics literature on certification seals and price premiums (see the second chapter of this dissertation for a more thorough review of the security literature). The second section discusses the hypotheses to be tested. Section three describes the data collected. The fourth section describes the results. After a variety of specifications and control variables were tried, I found a consistent relationship between website security (represented by the presence of security seals) and prices, and little to no evidence of a relationship between privacy and prices. Finally, the last section discusses implications of these results.

3.2 Literature

For a general overview of the economics and technical aspects of the protection of personal information, see Friedman (2009). Dranove and Jin (2010) provide a broad look at certification in general (i.e., not just online). Rubin and Lenard (2001) provide an overview of online privacy issues.

Little of the literature on online privacy and security is focused on investigating whether or not a price premium exists for sites that provide more privacy and security.

This is puzzling for two reasons:

- The existence of a price premium suggests that online markets have functioning mechanisms to protect personal information, and that regulations may be unnecessary.

- The lack of a price premium could mean that market mechanisms to protect personal information are not sufficient or efficient. It could also mean, however, that consumers do not value protecting their personal information very much.³⁶

Two papers look at the effect of certification seals on prices and influenced the course of this research. Baye and Morgan (2003) collect a panel of prices of 36 consumer electronics products from Shopper.com from November 1999 to May 2001, and examine whether sites with CNet certification charge a price premium. CNet certification was the most prominent form of differentiation on Shopper.com, and it required that firms satisfy various conditions regarding shipping costs, security, packaging, and other customer service-related issues (CNet certification still exists, but the seal does not show in Shopper.com listings; rather, all stores on the site are now certified). Baye and Morgan find that if only one seller has CNet certification, that seller enjoys a 5 percent price premium, but if other sites are also certified, the premium disappears. They do not consider any other certifications or seals because of their focus on Shopper.com prices. A 2004 paper by Baye, Morgan, and Scholten points out that there is a great deal of price dispersion in online markets. Although they explain much of the variation by differences in the number of firms listing prices, certification seals could be another explanation.

Nikitkov (2006) used data from eBay transactions to determine whether seals affect consumer behavior. The seals Nikitkov considers are not privacy or security-related; rather, they are what this paper refers to as “quality seals”—that is, they are seals

³⁶ This raises the question of why a site would incur the costs of obtaining seals. Such seals may not exist only to attract consumers. Another possible explanation could be that sites choose to pursue seals in order to follow best practices. That is, they may want to take advantage of the expertise a certifying entity provides, in order to, say, avoid costly customer service problems or legal trouble. Displaying the seal may be a signal to competitors, or may be expected to bring no benefit at all—but since it does not cost much to display the seal once certified, why not do so?

that suggest the seller is trustworthy and deals with customers quickly and fairly. The results are mixed. Seals do not appear to have an effect on whether or not an item is purchased at auction, or on the number of bidders. A Squaretrade seal does seem to raise the price at which auctioned goods sell. The number of bidders is included in the regression as an explanatory variable; its coefficient is positive and significant. It seems straightforward that if there is more interest in an auction, the price should be higher but this leads one to question why the additional bidders are participating. In a separate regression, the number of bidders seems unaffected by seals. Transactions involving a fixed price rather than an auction show mixed results, including a coefficient with the wrong sign (and significantly different from zero)—sellers with an excellent reputation on eBay charge a *lower* price in posted price sales (for which there is a simple fixed price, rather than an auction). The adjusted R-squares for the price regressions are low—.13—so there is a great deal of price variability left to explain. Nikitkov uses a price index to make price comparisons across different goods.

Certification seals and other security measures can suffer from a lemons problem—if users are unable to distinguish between seals that signal safety and seals that have weak verification procedures, then users do not trust the seals, and seals do not communicate information. Edelman (2009) has shown that sites with the TRUSTe seal are *less* likely to be trustworthy (as measured by spam, pop-ups, security exploits, scams, links to other bad sites, and other measures) than sites without the seal. Hadfield (2004) examines certification seals and their dispute resolution mechanisms in the context of the private provision of commercial law (like the Lex Mercatoria). Miyazaki and Krishnamurthy (2002) examine whether privacy and security seals such as TRUSTe and

BBBOnline provide useful information to consumers. They found that a minority of sites registered with these organizations post seals that are properly linked to the certifier's site. They also found that there was no significant difference between the privacy policies of sites with seals and those without. Paradoxically, they also conducted surveys which suggested that certification seals make consumers more at ease regarding their privacy. Rifon et al. (2005) use an online experiment and also find that consumers are comforted by the presence of seals, yet Larose and Rifon (2006) support Miyazaki and Krishnamurthy's skepticism of the value of seals, finding that sites without certification seals provided the same privacy assurances as sites with seals, *and* made fewer requests for personal information.

3.3 The Hypothesis To Be Tested

If some consumers care about protecting their personal information, and if it is costly for firms to provide that protection, then we should expect some firms to provide security, and some consumers to be willing to pay for it. If different firms provide different levels of security, then *the firms providing more security should charge higher prices* (in a market with differentiated products they may be attracting customers with a higher willingness to pay for security). Websites displaying privacy and security seals, such as TrustE and Verisign, should charge higher prices. This is similar to Nikitkov's hypothesis 2 (for which he found some supporting evidence in the case of eBay auctions).

There are many such seals; thirty four were found on the various websites used in this study (five more were found in an earlier stage of research, but they did not show up in this sample). I have divided the seals into three categories: privacy, security, and

quality (with a few seals covering more than one category). See Table 3.1 for this breakdown of seals. Privacy seals require that sites post a privacy policy and follow strict guidelines to protect personal information. Security seals are almost entirely focused on providing Secure Sockets Layer (SSL) encryption, which makes online transactions safer (by preventing third parties from being able to read data sent between the user and the site). Quality seals require that a site have a good reputation (often based on consumer-submitted reviews), respond quickly to consumer complaints, and generally keep consumers happy. Previous papers have focused on one or two seals at a time, yet consumers may see more seals as providing more security than fewer seals, or may see some seals as valuable and other seals as irrelevant.

I expand on Nikitkov's hypothesis by testing several variations on the basic "seals are associated with higher prices" idea. It is unclear *ex ante* how consumers will respond to seals. Is the mere presence enough, or are more seals better than fewer seals? Do consumers care more about common seals like Verisign, which are easily recognized? The following hypotheses are tested using several combinations of variables:

H1: Stores displaying a privacy seal have higher prices.

H2: Stores displaying a security seal have higher prices.

H3: Stores displaying a quality seal have higher prices.

H4: Stores displaying a larger number of privacy seals have higher prices.

H5: Stores displaying a larger number of security seals have higher prices.

H6: Stores displaying a larger number of quality seals have higher prices.

H7: Stores displaying seals that are more common have higher prices.

H8: Stores displaying a larger number of common seals have higher prices.

H9: Stores displaying specific seals have higher prices..

H10: Stores displaying a larger number of seals (of any kind) have higher prices.

I do not test Baye and Morgan's Red Queen hypothesis in this setting, because there is very little variation in certification seal variables over the nine week period (which also prevents estimation of firm-specific fixed effects). Therefore these results cannot tell us whether an advantage to one site conveyed by seals is merely temporary, and eliminated when other sites adopt seals.

If a relationship is not found, it does not necessarily imply that consumers do not value security, although that is one possibility. It is also possible that consumers do not see seals as a credible sign of security protection—perhaps credible seals are too costly for firms to provide.

3.4 Data

I selected 31 different goods for comparison of certification seal effects. These items, which are listed in Table 3.4, were picked from bestseller lists on sites such as Amazon.com and Buy.com. For each good, data was collected on variables specific to the websites selling them. Data on prices was collected from Google Product Search and Cnet Shopper using a custom-written application, and the thousands of seller listings were carefully screened by hand to ensure that each item was the one intended (so that, for example, the listed price was for the Batman Dark Knight Blu-ray disc, rather than the DVD or Collector's Edition). Pricegrabber and Pricewatch were also considered, but the

sellers were entirely redundant with the Google Product Search and Cnet Shopper results. Google Product Search is probably the largest product search engine, and Cnet Shopper was chosen because it was the subject of Morgan and Baye's previous study³⁷. The results of the analysis do not change substantially if the regressions are restricted to Google Product Search or Cnet Shopper data. Data from the two sources was combined³⁸, although the two listing services do differ in some regards. Both are free to sellers, but Cnet requires that sellers pass certification requirements, whereas Google Product Search takes any listing. Dummy variables for each time period and each good were created. Data on the presence or absence of seals and whether or not the site has the word "privacy" on the product page was collected by an application that searched through each site's page source. Sites with a link to the privacy policy on the front page may be placing a greater emphasis on privacy; the sign should be positive if this is meaningful and valuable to consumers. Table 3.3 contains the list of page source search terms.

The number of firms selling each product at each point in time was calculated as a measure of competition³⁹. Initially it was included as-is, with the expectation that more sellers would correlate with lower prices. Strangely, however, its coefficient was positive. After examining the data it was determined that this was probably due to "irrelevant"

³⁷ There are many other price search engines, including Bing Shopping, Shopping.com, and Yahoo Shopping. For a list of forty-two price search engines with some details on each, see here: <http://www.ecommercoptimization.com/comparison-shopping-listing-guide/>, last accessed 4-25-10.

³⁸ In some cases a store was listed selling an item in both Google Product Search and Cnet Shopper. Because the same store could not be listed twice at a given time, one of the listings was deleted. The criterion for deletion was to keep a listing that provided shipping costs, and if that did not eliminate one of the listings, then the higher-priced listing was eliminated. This criterion was seldom helpful, as prices from a particular store were almost always identical across search engines. In the remaining cases, the Cnet Shopper listing was used, due to their relative scarcity in the sample. Cnet Shopper listings are about 10% of the sample.

³⁹ Some sites, such as Amazon.com, appear in the sample more than once, because they are selling more than one of the items. Because this is a panel, this was dealt with by treating a store as a separate entity for each of the items sold—that is, when Amazon.com sells a cooking pot, it is considered a different store from when it sells a book.

price listings. Some sites selling in Google Product search seem to have non-competitive prices—prices at which no one would buy, given the option of reputable sellers at lower prices. Dividing the number of sellers into low, medium, and high categories seems to have resolved this problem. This is discussed further in the next section.

Finally, data on site reputation was collected from resellerratings.com by a custom application⁴⁰. Resellerratings.com allows consumers to rate retail websites based on their shopping experience. The overall rating provided by the site includes the consumer's opinion of the price, so in order to avoid endogeneity, I created a price-free rating, which averages the consumers' ratings for "Likelihood of Future Purchases", "Shipping and Packaging", and "Customer Service". A "Return or Replacement" category also exists, but I excluded it because many consumers did not have return or replacement experiences to rate. A third of the sites in the sample lack any rating on resellerratings.com. In order to avoid losing these observations, I split the ratings into No Rating, Low Rating, Medium Rating, and High Rating dummy variables, with the No Rating variable excluded. Therefore the coefficients for the Low, Medium, and High rating variables are all relative to sites that have no rating. Sites with higher ratings were expected to charge higher prices. The cutoff numbers for Low, Medium, and High were chosen so that roughly equal numbers of sites fell into each category.

These ratings are also useful in that they allow us to determine whether a quality seal has an affect that is separate from a site's reputation. That is, if a bizrate.com (for example) certification seal is significant and positive, it could mean that consumers see

⁴⁰ Data was also collected from resellerratings.com on the number of ratings a site received, but this was not used in the regressions in order to avoid introducing an identification problem. Sites with more ratings might have higher prices (supply) or lower prices (demand), but without an instrument to sort out which is which, the number of ratings is not useful.

the seal as a signal of quality, or it could mean that the seal (which in part means that consumers give the site positive ratings) is simply reflecting the site's reputation.

Including the ratings from resellerratings.com allows us to sort out these effects.

The certification seals variables were used to construct additional variables. Each seal is represented by a dummy variable, and these variables were summed to find the total number of seals for each site. It was expected that sites with more seals would charge higher prices. Variables were also created that measure the presence or absence of different types of seals (privacy, security, or quality), as well as the number of each type appearing. Again, the signs of these were expected to be positive—sites displaying seals, or displaying more seals, were expected to charge higher prices. Additionally, the frequency with which each seal occurred was used to create variables indicating the presence or absence of the five most common seals, as well as the presence or absence of the ten most common seals, and the number appearing in each category (Number of Top 5 and Number of Top 10). There are also dummy variables for each individual seal, such as Verisign or Truste or Scanalert; perhaps some of them are positively perceived by consumers, and others are not. As mentioned before, there is no way to know a priori whether consumers care about the mere presence of seals, or the number of seals, or the kinds of seals that appear, so it is necessary to test several possibilities.

The dependent variable in each regression is the natural log of the price of the item. Natural logs were taken (following Morgan and Baye 2003) in order to convert coefficients to percentage changes, to deal with the differences in the scale of price changes from item to item.⁴¹

⁴¹ Another advantage of using natural logarithms is dramatically better fit, compared to the price index used by Nikitkov (2006). Regressions were also estimated using a price index similar to Nikitkov's; each price

The variables are defined in Table 3.1 and summary statistics are provided in Table 3.2. There are 791 unique sites for the thirty-one items across nine one-week periods. There were also 104 additional stores that sold indirectly through other sites (for example, Buy.com selling through Amazon.com). These were excluded from the data in order to avoid confusion over which site was being measured (although rerunning the regressions with a dummy variable for indirect sales does not change any of the results, and the dummy variable is never significantly different from zero). Around two-thirds of the sites display the word “privacy” somewhere on their page, and more than half of them have some kind of seal. Privacy seals are relatively uncommon, appearing on around fifteen percent of the sites, while security seals appear on almost half the sites. I suspect that many of the seals used by sites are of dubious value; while some are common and well-known, such as Verisign, others, such as Digicert, are used by very few firms, and are unlikely to be recognized by consumers. On the other hand, perhaps such uncommon seals allow a site to distinguish itself. If the signs of the privacy coefficient and the seal coefficients are positive, this would provide strong support for the hypothesis that consumers value privacy and security and are willing to pay for them. A small number of sites did not respond to the application that searches page sources for phrases⁴². The sample sizes exceed 8,500 observations in all regressions.

During the initial stages of this research, Firefox and Google Chrome were used to verify that prices of six test products were the same for all websites, regardless of

was normalized to the average price for that good during the same time period, allowing comparison across goods. Regressions run using this dependent variable had nearly zero explanatory power, and are not included in this paper.

⁴² A manual check of these pages revealed that they did not load at all, despite their appearance in Google Product Search or CNet Shopper. They may have closed down, and it seems that one of the sites might have been a scam.

browser or cookies. Chrome has an “incognito mode” which prevents storage of cookies or other information, making it difficult for a site to gather information about a consumer. A small random sample of sites was also checked for consistency of prices when shopping with and without an account. That is, if a site required an account to getting shipping costs, I created a false account, and then verified that the price was the same with and without an account. The purpose of this was to determine whether or not any sites were using cookies or other information to price discriminate. In no case did any price change; no evidence of price discrimination was found. A more thorough study of this subject would require creating accounts at these sites and actually buying things to create a purchase history, but this is beyond the scope of this project. At the moment, there remains no evidence that sites engage in cookie or purchase-history based price discrimination.

3.5 Estimation Technique and Results

Panel Data regressions with Random Effects were estimated (Fixed Effects could not be estimated because of the lack of change over time in the explanatory variables). Tables 3.5 through 3.8 provide the results of the individual regressions, but they omit the time and item dummy variable coefficients (because they are not economically significant and because they reduce readability, although they are nearly all statistically significantly different from zero). The general form of the equation estimated is:

$$\ln(\text{Price}_{it}) = \alpha_1 + \alpha_{2i} + \alpha_{3t} + \beta(\text{Certification Seal Variables}_{it}) + \varepsilon_{it} + u_i$$

Where β is a vector coefficients that are expected to be positive.

The results suggest that certification seals positively affect prices, particularly security seals; this will be discussed in detail as the regressions are discussed one by one below. The non-seal variables have similar coefficients and significance from regression to regression. The variable “privacy”, which indicates the presence of that word on the page somewhere (and suggests the existence of a privacy policy) is never statistically significant. Relative to sites in markets with low competition (less than five firms), firms in markets with medium (five to nineteen firms) or high competition (twenty or more firms) charge significantly lower prices, and the difference between medium and high competition is not significant. Sites with medium (from four up to seven on a ten point scale) and high (from seven to ten on a ten point scale) ratings by consumers on resellerratings.com charge significantly *lower* prices, which is a surprising result. It is similar to the result in Nikitkov, that fixed-price sales on eBay have higher prices when the seller has a better reputation. The reason for this result merits further investigation in future work. It could have to do with economies of scale that are complementary with customer service. If the resellerratings.com variables are excluded, the quality seal variables become significant in some regressions, suggesting that they are really picking up the effect of consumer ratings that allow such seals, rather than being of independent importance to consumers. It is also possible that consumers who are attracted to sites with the lowest prices are less concerned about the other aspects of retailer quality, or that once a consumer gets a low price, they are satisfied and simply give a site a pass on other aspects of retailer quality.

The regressions are ordered from the crudest to the most elaborate. Regression 1 looks only at the total number of seals on a site. Adding a seal correlates with a 1%

increase in the price, and this is significant at the 1% level. It is prudent to be skeptical of this result, as so many of the seals are security seals. Adding another seal is very similar to adding another security seal, and this is borne out by the magnitude of the coefficient—around 1%, similar to the coefficient of “Number of Security Seals” in regressions 2 and 4. This regression provides some support for H10.

Regression 2 is slightly more complex, in that it considers individual seals, such as Scanalert and Verisign, to determine if some matter while others do not. The seals are listed in order of frequency, that is, Scanalert is the most common seal, and controlscan is the least common. The scanalert seal (a security seal) is significant at the 10% level, and the buysafe seal (a quality seal) and controlscan seal (a security seal) are significant at the 5% level. All have positive coefficients, but it is hard to reconcile these results with the other results. Most of the security seals have, individually, no effect, yet the other regressions suggest that security seals should matter, or that the top ten seals should matter. It is hard to understand why consumers would pay a price premium for security seals in general, but not for specific security seals. Regression 7 provides some support for H9.

Regressions 3 and 4 are fundamental; they examine whether the existence or number of different kinds of seals matter. The certification seal variables show a consistent pattern. Sites that display security seals (regression 3) have significantly higher prices, and the more security seals they display, the higher the price (regression 4). An additional security seal correlates with slightly more than a 1% increase in price. Privacy and quality seals do not seem to matter. In terms of hypotheses H1 through H10, regression 1 supports H2, while regression 2 supports H5. Compare this with the 5%

premium found to be enjoyed by Amazon (simply for being Amazon) relative to Barnesandnoble.com found by Clay et al. (2002). The security premium seems small, but thought of another way, a security seal gets a site a fifth of the way to having Amazon's price premium.⁴³

Regressions 5 through 8 add variables examining the frequency with which seals occur. Adding variables for the number (regressions 5 and 6) or existence (regressions 7 and 8) of the five most common and ten most common seals muddies the picture somewhat. If "Top 5" variables are included, security seals are still significant and positive, while the "Top 5" variables are not significant. Again, an additional security seal correlates with slightly more than a 1% increase in price. If "Top 10" variables are included, security seals are no longer significant, and the "Top 10" variables become significant at the 10% level. Six of the top ten seals are security seals (and one of them, bbb.org, covers security, quality, and privacy), so there could simply be multicollinearity, but with a sample size this large, this should not be a problem. If one excludes the quality, security, and privacy seal variables, the "Top 5" and "Top 10" variables are both significant and positive (but these regressions are not reported here). Regressions 5 and 7 support H5 and H2, respectively, while 6 and 8 support H7 and H8.

To summarize these results, there are several regressions suggesting that security seals matter, correlating with price premiums around 1%. No regressions support hypotheses H1, H3, H4, or H6, so we may infer that quality and privacy seals do not correlate with a price premium. There is some support for H7 and H8; more popular seals (in the form of Top 5 Seals, but not Top 10 Seals) *may* allow a premium (presumably

⁴³ Whether Amazon still enjoys such a price premium is unclear. In the sample used in this paper, Amazon charges prices five to ten percent *lower* than the mean.

because consumers actually recognize them). H9 and H10 have some support in regressions 1 and 2, but it is possible that these regressions are really picking up the effect of security seals.

In each case, the R-square of the regression is very high—above 0.97. Simply including the time and item dummy variables is enough to explain nearly all the variation in prices; there is not much variation in the dependent variable left for seal-related variables to explain. Most of the additional variables are persistently significant, nonetheless.

Several variations on these regressions were tested to check for robustness. The results are not reported here in tabular form, but they included:

- Separate regressions for data from Google Product Search and Cnet Shopper. The results did not change for Google Product Search. The Cnet Shopper data gave different results, but the limited size of the Cnet Shopper sample (851 observations) suggests the results should be viewed skeptically. Leaving the Cnet Shopper data out of the regressions presented in tables in this paper does not change the results.
- Regressions based on product type—i.e., one for electronics, one for books, etc. The results were similar.
- Including shipping costs (when available; the shipping method was not controlled for due to lack of information). This reduces the sample size to less than 3,000 observations, but security seals still correlate with a higher prices.
- Regressions based on price range. Several different price ranges were tried, with no change in results, with one exception. When the sample was restricted to

goods priced from \$80 to \$200, security seals ceased to be significant. Why this would be the case is unclear; the subsample contains 2,221 observations.

3.6 Discussion

The strength of the results is surprising, given the previous papers in this area. Nikitkov (2006) also found that seals positively affect prices, but the regressions had little explanatory power overall. Baye and Morgan (2003) found that seals only matter so long as other sites do not adopt them, although they only considered one seal, and they focused on a setting in which that single seal was, for consumers, a low-cost source of information. That is, in both cases, the search engine results immediately informed consumers of the presence or absence of a seal, unlike the sites in this dataset, for which consumers must go to the actual webpage to see the seals.

This paper's innovation is the large amount of data on website characteristics collected. From regression to regression, seals repeatedly seem to matter, particularly security seals. This is a novel result, and it can be argued that it is a sensible one. Privacy, despite the attention paid to it, may not be as vitally important to consumers as security. Even if a website did collect and sell a user's personal information, it would likely be sold to a firm that wants aggregate data. Such firms do not care about the individual so much as the pattern of data the individual represents. What kinds of products does he or she buy, and how often? In what part of the country does he or she live? How old is the customer? This information is useful for making marketing decisions; it is unlikely to be used to harm the consumer. It may even result in advertisements that are more relevant to consumers in general, and may *benefit* this consumer. Online shopping may be safe

enough that privacy concerns do not deter buyers. Although early survey results (such as Kovar et al., 2000) suggested consumers wanted more privacy, these results should be viewed skeptically. When asked “do you want more of a good or less of a good,” (such as privacy) consumers are likely to say “more” if they are not asked to pay for it.

Security, however, is of much more immediate importance to the consumer. Someone who intercepts personal information as it is transmitted to the seller is surely up to no good, and may be planning to use credit card information or commit some other form of identity theft. It is easy to imagine that consumers would pay a one percent premium to ensure their personal information is transmitted securely. It is possible that some third factor is driving both security seals and prices, rather than security seals being a factor that allows a site to charge higher prices.

A priori arguments for quality seals are less clear. There are other ways of getting information about the trustworthiness of a site, such as going to reselleratings.com directly, or using Google Product Search to look up a seller’s reputation. There may be less measureable indicators of quality, such as a site’s layout, and word-of-mouth reputation. In any case, quality seals do not have a clear relationship with prices in these regressions.

Future studies should fill the gaps between the current studies. It may be valuable to test the Red Queen effect for a large number of seals (rather than just one) over an extended time period. Perhaps analysis of the use of other seals on eBay would provide stronger results. A focus on privacy-sensitive goods, such as pornography, drug paraphernalia, or weaponry might provide different results.⁴⁴ It would also be interesting

⁴⁴ Guns were also considered for this paper, but there are too few online vendors. Drug paraphernalia might be privacy-sensitive, but it is difficult to find a product sold without differentiation across many sellers.

to look over a longer timespan so that there is more variation in the seals across time. Finally, the negative correlation between prices and consumer ratings deserves investigation.

3.7 Conclusions

I have found evidence from a large panel of online retailers that seals displayed on retail websites allow these sites to charge a price premium, particularly in the case of security seals. Privacy seals and quality seals do not display a robust effect. This suggests that security may be more important to consumers than privacy.

Table 3.1: Variable Definitions

Dependent Variable:	Description:
price	The listed price for one of the thirty one goods studied at a particular store and date.
ln(price)	The natural log of the price.

Seal Variables:	Description:	Seal Type:
Authorize.net merchant verified	Equals one if the site has an Authorize.net merchant verified seal.	Security
Bizrate.com customer certified	Equals one if the site has a Bizrate.com Customer Certified seal.	Quality
BBB.org	Equals one if the site has a BBBOnline Reliability Seal.	Privacy, Quality
Buysafe	Equals one if the site has a buysafe seal.	Quality
Cnetcertifiedstore	Equals one if the site has a Cnet Certified Store seal.	Security, Privacy, Quality
Comodo	Equals one if the site has a Comodo seal.	Security
Controlscan	Equals one if the site has a Controlscan seal.	Security
Cybersource	Equals one if the site has a CyberSource Protected Buy seal.	Security
Cybertrust	Equals one if the site has a Cybertrust seal.	Security
Digicert	Equals one if the site has a Digicert seal.	Security
Dnb.powerprofiles.com	Equals one if the site has a Dun and Bradstreet Listed seal. This seal does not seem to guarantee anything related to security, privacy, or quality.	
Geotrust	Equals one if the site has a Geotrust seal.	Security
Godaddysecurewebsite	Equals one if the site has a GoDaddy Secure Website seal.	Security
Internet Retailer Top 500	Equals one if the site has an Internet Retailer Top 500 seal.	Quality
Mcafeesecure	Equals one if the site has a McAfee	Security

	Security seal.	
Nextagtrustedseller	Equals one if the site has a NexTag Trusted Seller seal.	Quality
Paypalverified	Equals one if the site has a PayPal Verified seal.	Security
Rapidssl	Equals one if the site has a RapidSSL seal.	Security
Ratepoint	Equals one if the site has a Rate Point seal.	Quality
Reseller Rating Award	Equals one if the site has a Reseller Rating Award seal.	Quality
Safe Shopping Network	Equals one if the site has a Safe Shopping Network seal.	Security
Scanalert	Equals one if the site has a ScanAlert seal.	Security
Shopping.com	Equals one if the site has a Shopping.com seal.	Quality
ShopWiki	Equals one if the site has a ShopWiki seal.	Security, Quality
Thawte	Equals one if the site has a Thawte seal.	Security
Truste	Equals one if the site has a Truste seal.	Privacy
Trustwave	Equals one if the site has a trustwave seal.	Security
Verisign	Equals one if the site has a Verisign seal.	Security
Visa	Equals one if the site has a Visa security seal (note that this is <i>not</i> the same as having a seal showing that a site accepts Visa as payment).	Security
Volusion SSL	Equals one if the site has a Volusion SSL seal.	Security

Other Seal-related Variables:	Description:
Displays a Top 5 Seal	Equals one if the site has one of the five most common seals.
Displays a Top 10 Seal	Equals one if the site has one of the ten most common seals.
Number of Top 5 Seals	The number of top five seals most common seals

	appearing on a site.
Number of Top 10 Seals	The number of top ten seals most common seals appearing on a site.
Displays a Privacy Seal	Equals one if a site displays a privacy seal.
Displays a Security Seal	Equals one if a site displays a security seal.
Displays a Quality Seal	Equals one if a site displays a quality seal.
Number of Privacy Seals	The number of privacy seals displayed on a site.
Number of Security Seals	The number of security seals displayed on a site.
Number of Quality Seals	The number of quality seals displayed on a site.
Total Number of Seals	This is the sum of the columns of seal dummy variables for a particular store. The idea is that the more seals there are, the better security and privacy protection might be.

Other Variables:	Description:
Privacy	Equals one when the product page contains the word “privacy” somewhere (usually linking to a privacy policy page).
Resellerrating.com Low Price-Free Lifetime Rating	An average of three categories of consumer ratings of each retail site. “Lifetime” means that the rating is the average over the entire time the site has been on resellerratings.com; a six month rating was also available but not used as it reduced the sample size. “Low” means that the rating was less than 4 (with zero being the lowest possible rating).
Resellerrating.com Medium Price-Free Lifetime Rating	An average of three categories of consumer ratings of each retail site. “Lifetime” means that the rating is the average over the entire time the site has been on resellerratings.com; a six month rating was also available but not used as it reduced the sample size. “Medium” means that the rating was 4 or higher, but less than 7.
Resellerrating.com High Price-Free Lifetime Rating	An average of three categories of consumer ratings of each retail site. “Lifetime” means that the rating is the average over the entire time the site has been on resellerratings.com; a six month rating was also available but not used as it reduced the sample size. “High” means that the rating was 7 or higher (with 10 being the highest possible rating).
Low Competition	A dummy variable equal to one if there are five or

	fewer firms selling a particular good at that time.
Medium Competition	A dummy variable equal to one if there are more than five but less than 21 firms selling a particular good at that time.
High Competition	A dummy variable equal to one if there are more than twenty firms selling a particular good at that time.

Table 3.2: Summary Statistics

	Mean	Standard Deviation	Minimum	Maximum	Sum of observations
Price	176.89	138.71	4.61	799.99	NA
ln(Price)	4.79	0.97	1.53	6.68	NA
Cnet Shopper Listing	0.10	0.30	0	1	851
Privacy	0.73	0.44	0	1	6237
verisign	0.17	0.37	0	1	1412
controlScan	0.02	0.13	0	1	149
truste	0.08	0.27	0	1	651
dnb.powerprofiles.com	0.00	0.06	0	1	31
thawte	0.04	0.19	0	1	328
bbb.org	0.10	0.30	0	1	853
mcafee	0.11	0.31	0	1	945
scanalert	0.25	0.44	0	1	2157
buysafe	0.02	0.13	0	1	150
authorize.net	0.07	0.26	0	1	631
instantssl	0.02	0.14	0	1	160
comodo	0.04	0.19	0	1	303
ratepoint	0.00	0.06	0	1	35
geotrust	0.04	0.21	0	1	377
bizrate	0.14	0.34	0	1	1155
cnet.com	0.03	0.18	0	1	278
trustwave	0.03	0.16	0	1	238
nextag.com	0.03	0.17	0	1	249
square trade	0.00	0.03	0	1	8
PayPal Verified	0.01	0.08	0	1	50
Security Metrics	0.00	0.04	0	1	13
seal.godaddy.com	0.03	0.18	0	1	292
RapidSSL	0.01	0.10	0	1	93
VisaVerified	0.00	0.07	0	1	42
cybersource	0.03	0.18	0	1	280
shopping dot com	0.00	0.07	0	1	38
Internet Retailer Top 500	0.01	0.11	0	1	113
resellerratings	0.06	0.24	0	1	507
cybertrust	0.02	0.13	0	1	140
sortprice	0.02	0.15	0	1	196
Shopwiki certified price	0.01	0.10	0	1	82

leader					
safeshoppingnetwork	0.00	0.06	0	1	29
digicert	0.00	0.05	0	1	19
volusion	0.01	0.12	0	1	116
Total Seals	1.42	1.58	0	8	12120
Number of Apparent Sellers	42.84	18.75	1	77	NA
DisplaysTop 5	0.43	0.49	0	1	3650
Displays Top 10	0.52	0.50	0	1	4470
Number of Top 5	0.77	1.03	0	4	6522
Number of Top 10	1.06	1.26	0	6	9016
Displays Privacy Seal	0.17	0.38	0	1	1451
Displays Security Seal	0.48	0.50	0	1	4120
Displays Quality Seal	0.27	0.44	0	1	2309
Number of Privacy Seals	0.21	0.50	0	3	1782
Number of Security Seals	0.78	0.99	0	5	6667
Number of Quality Seals	0.41	0.77	0	4	3460
Reseller Rating-6 month rating	5.38	3.35	0	10	25268
Reseller Rating-lifetime rating	6.27	2.66	0	10	34925
Reseller Rating-6 month count	76.87	248.39	0	1926	462234
Reseller Rating-lifetime count	932.36	3711.41	0	30965	5606268
Reseller Rating-price-free rating	4.92	3.11	0	10	23083
Low Competition	0.01	0.08	0	1	50
Medium Competition	0.18	0.38	0	1	1518
High Competition	0.82	0.39	0	1	6956
Reseller Rating Low Price-Free Rating	0.16	0.37	0	1	1375
Reseller Rating Medium Price-Free Rating	0.15	0.36	0	1	1267
Reseller Rating High Price-Free Rating	0.16	0.37	0	1	1364

Table 3.3: Page Source Search Terms

privacy
verisign
siteSafe
controlScan
truste
dnb.powerprofiles.com
carbonfree
thawte
bbb.org
mcafee
scanalert
buysafe
authorize.net
instantssl
comodo
publiceye
ratepoint
geotrust
bizrate
cnet.com
trustwave
nextag.com
square trade
PayPal Verified
Security Metrics
seal.godaddy.com
RapidSSL
VisaVerified
cybersource
shopping dot com
my simon
Internet Retailer Top 500
resellerratings
cybertrust
sortprice
Shopwiki certified price leader
safeshoppingnetwork

digicert
volusion
hacker guard

Table 3.4: Items and Their Product Categories

Item Number	Item Description	Category
1	Sapphire Radeon HD 5770 video card	Computers
2	BFG Nvidia Geforce GTX 295 video card	Computers
3	Dewalt Cordless Drill kit DC720KA	Household Tools
4	Freakonomics, revised and expanded, hardcover	Books
5	The Undercover Economist, paperback	Books
6	True Compass, hardcover	Books
7	Intel Core i7-920 retail CPU	Computers
8	Intel Core 2 Quad Q9400 retail CPU	Computers
9	AMD Black Edition Phenom 965 125 Watt retail CPU	Computers
10	Garmin nüvi 255W GPS Navigator	Electronics
11	Flip UltraHD Camcorder, 120 Minutes, Black	Electronics
12	Canon Powershot G10 digital camera	Electronics
13	Asus eee PC 1005HA-PU1X-BK N280 netbook computer	Computers
14	Onkyo TX SR607 receiver, black	Electronics
15	Sony Bravia Theater DAV-HDX589W Home theater system	Electronics
16	Yamaha EZ200 keyboard	Musical Instrument
17	Takamine S35 Jasmine Guitar	Musical Instrument
18	The Lost Symbol, hardcover	Books
19	Black Decker GH1000 string trimmer	Household Tools
20	Hoover U5140-900 Tempo Upright Vacuum Cleaner	Household Tools
21	Hamilton Beach 33967 cooker	Household Tools
22	Furminator large yellow deshedding tool with 4-inch edge	Household Tools
23	Hannah Montana "The Movie" DVD	Movies
24	Monsters vs. Aliens DVD	Movies
25	The Dark Knight Blu-Ray	Movies
26	The Big Bang Theory Complete Second Season DVD	Movies
27	The Wizard of Oz blu-ray 70th anniversary	Movies
28	Halo 3 ODST Xbox 360 game	Video Games
29	Uncharted 2: Among Thieves, Playstation 3 game	Video Games
30	Nintendo Wii video game console	Video Games
31	Brother HL-2140 Personal Laser Printer	Computers

Table 3.5: Regression 1:

VARIABLES	(3) lnprice
Privacy	-0.00898 (0.00836)
Medium Competition	-0.0439*** (0.0145)
High Competition	-0.0421*** (0.0151)
Reseller Rating Low Price-Free Rating	-0.0166 (0.0135)
Reseller Rating Medium Price-Free Rating	-0.0453*** (0.0137)
Reseller Rating High Price-Free Rating	-0.0645*** (0.0138)
Total Seals	0.00934*** (0.00239)
Constant	5.279*** (0.0456)
Time and Item Dummies Included	Yes
Observations	8509
Number of store/item combinations	1546

Note: Time and item dummy variables are nearly all statistically significant in every regression, but are omitted from the tables for readability.

Table 3.6: Regression 2:

VARIABLES	(8) lnprice
Privacy	-0.01000 (0.00854)
scanalert	0.0204* (0.0115)
verisign	-0.00803 (0.0131)
bizrate	-0.00437 (0.0103)
mcafee	0.0193 (0.0130)
bbborg	0.0107 (0.0117)
truste	0.0176 (0.0134)
authorizenet	0.0196 (0.0198)
resellerratings	0.0207 (0.0158)
geotrust	0.00948 (0.0177)
thawte	0.00204 (0.0208)
comodo	-0.00642 (0.0261)
sealgodaddycom	0.00956 (0.0223)
cybersource	0.0144 (0.0231)
cnetcom	0.00561 (0.0231)
nextagcom	-0.0166 (0.0286)
trustwave	-0.0270 (0.0333)
sortprice	0.0219

	(0.0254)
instantssl	-0.0239
	(0.0410)
buysafe	0.0738**
	(0.0360)
controlscan	0.0802**
	(0.0329)
Medium Competition	-0.0439***
	(0.0145)
High Competition	-0.0418***
	(0.0151)
Reseller Rating Low Price-Free Rating	-0.0147
	(0.0138)
Reseller Rating Medium Price-Free Rating	-0.0462***
	(0.0141)
Reseller Rating High Price-Free Rating	-0.0571***
	(0.0144)
Constant	5.282***
	(0.0457)
Time and Item Dummies Included	Yes
Observations	8509
Number of store/item combinations	1546

Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 3.7: Regressions 3 and 4:

VARIABLES	(1) lnprice	(2) lnprice
	(0.0477)	(0.0477)
Privacy	-0.00738	-0.00790
	(0.00843)	(0.00832)
Medium Competition	-0.0440***	-0.0438***
	(0.0145)	(0.0145)
High Competition	-0.0424***	-0.0422***
	(0.0151)	(0.0151)
Reseller Rating Low Price-Free Rating	-0.0142	-0.0144
	(0.0135)	(0.0135)
Reseller Rating Medium Price-Free Rating	-0.0419***	-0.0424***
	(0.0137)	(0.0138)
Reseller Rating High Price-Free Rating	-0.0582***	-0.0624***
	(0.0137)	(0.0140)
Displays Privacy Seal	0.0139	
	(0.00983)	
Displays Security Seal	0.0172**	
	(0.00753)	
Displays Quality Seal	-0.00241	
	(0.00785)	
Number of Privacy Seals		0.00940
		(0.00873)
Number of Security Seals		0.0117***
		(0.00372)
Number of Quality Seals		-0.00129
		(0.00619)
Constant	5.276***	5.276***
	(0.0457)	(0.0457)
Time and Item Dummies Included	Yes	Yes
Observations	8509	8509
Number of store/item combinations	1546	1546

Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 3.8: Regressions 5, 6, 7, and 8:

VARIABLES	(5) lnprice	(6) lnprice	(7) lnprice	(8) lnprice
privacy	-0.00931 (0.00844)	-0.00973 (0.00838)	-0.00754 (0.00846)	-0.00754 (0.00843)
Medium Competition	-0.0438*** (0.0145)	-0.0439*** (0.0145)	-0.0440*** (0.0145)	-0.0443*** (0.0145)
High Competition	-0.0420*** (0.0151)	-0.0422*** (0.0151)	-0.0424*** (0.0151)	-0.0429*** (0.0151)
Reseller Rating Low Price-Free Rating	-0.0157 (0.0135)	-0.0170 (0.0135)	-0.0144 (0.0135)	-0.0154 (0.0135)
Reseller Rating Medium Price- Free Rating	-0.0428*** (0.0138)	-0.0433*** (0.0138)	-0.0420*** (0.0138)	-0.0432*** (0.0137)
Reseller Rating High Price-Free Rating	-0.0624*** (0.0140)	-0.0629*** (0.0140)	-0.0583*** (0.0137)	-0.0572*** (0.0137)
Displays Privacy Seal			0.0139 (0.00983)	0.00904 (0.0102)
Displays Security Seal			0.0165** (0.00816)	0.00722 (0.00919)
Displays Quality Seal			-0.00387 (0.0101)	-0.00862 (0.00851)
Number of Privacy Seals	0.00805 (0.00883)	0.00317 (0.00938)		
Number of Security Seals	0.0107*** (0.00387)	0.00626 (0.00481)		
Number of Quality Seals	-0.00446 (0.00700)	-0.00743 (0.00707)		
Number of Top 5	0.00477 (0.00491)			
Number of Top 10		0.00997* (0.00554)		
Displays Top 5			0.00232 (0.0101)	
Displays Top 10				0.0173* (0.00912)
Constant	5.277*** (0.0457)	5.278*** (0.0456)	5.277*** (0.0457)	5.277*** (0.0457)
Time and Item Dummies Included	Yes	Yes	Yes	Yes
Observations	8509	8509	8509	8509

Number of store/item combinations	1546	1546	1546	1546
-----------------------------------	------	------	------	------

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

References

- Baye, M., J. Morgan, and P. Scholten (2004). "Price Dispersion in the Small and in the Large: Evidence from an Internet Price Comparison Site," *The Journal of Industrial Economics*, 51(4): 463-507.
- Baye, M., and J. Morgan (2003). "Red Queen Pricing Effects in E-Retail Markets." SSRN Working Paper #655448.
- Clay, K., R. Krishnan, E. Wolff, and D. Fernandes (2002). "Retail Strategies on the Web: Price and Non-Price Competition in the Online Book Industry," *The Journal of Industrial Economics*, L (3): 351-367.
- Dranove, D., and G. Jin. (2010) "Quality Disclosure and Certification: Theory and Practice." NBER Working Paper #w15644.
- Edelman, B. (2009). "Adverse Selection in Online "Trust" Certifications." *Proceedings of The 11th International Conference on Electronic Commerce*.
- Friedman, D.. (2009) *Future Imperfect*. New York: Cambridge University Press.
- Hadfield, G. (2004) "Delivering Legality on the Internet: Developing Principles for the Private Provision of Commercial Law," *American Law and Economics Review* 6 (1), 154-184.
- Kovar, S., K. Burke, and B. Kovar (2000). "Consumer Responses to the CPA WEBTRUST Assurance," *Journal of Information Systems* 14 (1), 17-35.
- Larose, R., and N. Rifon (2006) "Your Privacy is Assured – of Being Disturbed: Websites With and Without Privacy Seals." *New Media & Society*, 8(6): 1009-1029.
- Miyazaki, A., and S. Kirshnamurthy (2002) "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions." *The Journal of Consumer Affairs*,

Nikitkov, A. (2006) "Information Assurance Seals: How they Impact Consumer Purchasing Behavior." *Journal of Information Systems*, 20(1): 1-17.

Rifon, N., R. Larose, and S. Choi (2005) "Your Privacy is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures." *The Journal of Consumer Affairs*, 39(2): 339-362.

Rubin, P., and T. Lenard (2001) "Privacy and the Commercial Use of Personal Information." Progress and Freedom Foundation monograph.