No. 12-05
January 2012

WORKING PAPER

IS THERE A CYBERSECURITY MARKET FAILURE?

By Eli Dourado

Is There a Cybersecurity Market Failure?

Eli Dourado

elidourado@gmail.com

Working Paper

December 14, 2011

1. Introduction

Computer networking is a young and rapidly evolving technology. Consequently, observers are still grappling with the implications that the Internet and related technologies will have for our lives. The uncertainty, the order amidst chaos, and the perpetual change entailed by an important technology in flux have led policy makers to be vigilant in assessing the threats and policy issues raised by the maturation of the Internet. This vigilance in turn has expanded into calls for political and regulatory action in a number of entangled domains collectively called cybersecurity.

Vigilance within reason is good;[1] nevertheless, it must be matched by a good sense of what constitutes a justification for action. One widely accepted rationale for government intervention is what economists call market failure, and proponents of government intervention in cybersecurity have rested their case primarily on this basis. The Center for Strategic and International Studies (CSIS) argues in a report aimed at the 2009 presidential transition, "It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives."[2] James A. Lewis, director of the Technology and Public Policy Program at the CSIS, argued in congressional testimony,

> [A]bsent government intervention, security may be unachievable. Two ideas borrowed from economics help explain this—public goods and market failure.

---

[1] The optimal amount of vigilance is that which generates expected marginal benefits equal to marginal cost. Consequently, there can be such a thing as too much vigilance. For purposes of this paper, however, I will not question the amount of vigilance directed toward cybersecurity; my quarrel is solely with the subsequent economic reasoning.

[2] Center for Strategic and International Studies (CSIS), CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency* (Washington, DC: CSIS, December 2008), 50, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

> Public goods are those that benefit all of society but whose returns are difficult for any individual to capture. Basic research is one public good that the market would not adequately supply if government did not create incentives. Cybersecurity is another such public good where market forces are inadequate.[3]

In their alarmist 2010 book, *Cyber War*, Clarke and Knake refer to the existence of market failure in passing without any further elaboration.[4] Van Eeten and Bauer write,

> If the incentives of the players in the value net do not properly reflect the social costs and benefits of their security decisions, for example, because of externalities or public good aspects of security investments, such privately rational decisions will systematically deviate from the social optimum. Insufficiently low security investments may manifest in slower diffusion rates of IT uses and the associated opportunity costs to society."[5]

Since the justification for regulatory intervention in cybersecurity rests primarily on the charge of market failure, it is worth carefully investigating whether the alleged market failures exist. A market failure exists when, in an unfettered market, there exists in principle a trade that *could occur* between market participants that would make at least one participant better off and no participant (or bystanders) worse off, which *does not occur*. If we courageously assume that government intervention will make beneficial trades occur in missing markets without additional distortion, then it is hard to object to the use of this standard in policy analysis. Yet identifying

---

[3] U.S. Senate Committee on Commerce, Science, and Transportation, Hearing 111-667, testimony of James A. Lewis, February 23, 2010, http://www.gpo.gov/fdsys/pkg/CHRG-111shrg57888/html/CHRG-111shrg57888.htm.
[4] See, e.g., Richard A. Clarke, and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 137.
[5] Michel Van Eeten and Johannes M. Bauer, "Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications," *Journal of Contingencies and Crisis Management* 17 (December 2009): 223.

market failures is difficult. The task is to identify something that *does not happen*, that is, which is not observable. At best, market failure can be inferred.

One popular source of alleged market failures is the concept of externality, a cost or benefit incurred by a bystander. For instance, consider fans at a baseball stadium. A player hits a ball deep into the outfield, and the fans are eager to see if it will be a home run. To get a better view, one fan stands up. This worsens the view of the fan seated directly behind him. That fan also stands up for a better view, as does the fan in the next row, and so on. In equilibrium, we will observe all the fans standing up, each with a view no better than if he or she were seated. If we assume that, other things equal, fans prefer to sit than to stand, then we can infer a market failure.[6] Fans would be better off if they could agree not to stand to get a better view during the exciting moments of the game. The market failure is driven by the externality: the deterioration of the seated fans' view when some fans stand up.

Some policy analysts seem willing to infer a market failure any time they observe an externality. This inference is a colossal error. Despite the close relationship between externalities and market failure, the observation of an externality is *not sufficient* to infer a market failure. This paper is devoted to the rectification of this error, with specific application to cybersecurity policy. The first half of the paper presents several reasons, supported by the economic literature, why externalities are insufficient for the inference of market failure. The second half of the paper applies these arguments to areas of cybersecurity policy in which it has been claimed that markets have failed and government intervention is therefore necessary. This paper finds that alleged cybersecurity market failures are, at a minimum, much smaller than they at first appear

[6] It is not obvious that fans do prefer to sit than to stand during the exciting moments of the game. Some have been observed to rise in excitement even when watching sports on television, when standing could confer no sight advantage.

and, consequently, that attempts to correct them through naïve government regulation run the serious risk of doing more harm than good.

2. Externalities and Market Failure

This section explores several arguments for why market failure cannot be immediately inferred from the observation of externalities. The arguments include simple Coasian internalization, complex Coasian internalization, informal solutions to externality problems, and the case of inframarginal externalities.

Simple Coasian Internalization

In a pair of papers more than half a century old, Ronald Coase demonstrates that the presence of externalities is not sufficient to establish the existence of market failure. In "The Federal Communications Commission," Coase argues that the interference generated by adjacent positions on the licensed radio spectrum, a clear externality, would be easily internalized if property rights for the spectrum were well-defined.[7] Broadcasters could pay owners of adjacent spectrum licenses not to broadcast, or they could purchase the adjacent spectrum themselves. In this way, the highest-value broadcasts would proceed without interference, or with only the efficient level of interference. In "The Problem of Social Cost," Coase discusses his insight and its limitations in more general terms.[8] Because Coase's nuanced argument has been frequently

[7] Ronald Coase, "The Federal Communications Commission," *Journal of Law and Economics* 2 (October 1959): 1–40.
[8] Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3 (October 1960): 1–41.

misinterpreted and used as a straw man,[9] this paper will present in this section the case of "simple" Coasian internalization of externalities and in the next section the "complex" case.

Coase emphasizes the reciprocal nature of externalities:[10]

> The traditional approach [to externality problems] has tended to obscure the nature of the choice that has to be made. The question is commonly thought of as one in which A inflicts harm on B and what has to be decided is: how should we restrain A? But this is wrong. We are dealing with a problem of a reciprocal nature. To avoid the harm to B would inflict harm on A. The real question that has to be decided is: should A be allowed to harm B or should B be allowed to harm A? The problem is to avoid the more serious harm.

If by inflicting $5 of harm on A, B gains $10, then it is efficient for B to continue to harm A. For if B were prohibited from harming A, he would lose $10, while A would gain only $5. Society as a whole is better off if B harms A than if A harms B. Consequently, it is efficient for some externalities to persist uncorrected. The goal of policy should not be to eradicate all externalities indiscriminately.

It can be difficult to tell by mere observation if a given externality is efficient or inefficient. To do so, one would have to observe the amount gained or lost by each party from the externality. This may be impossible. Even if these gains and losses can be identified, the options available to each party for mitigating the harm are not always clear. There may be cheap alternatives to emitting some kinds of pollution, or there may be relatively cheap ways for bystanders to live with pollution. The efficient resolution of the externality problem requires that

---

[9] Butler and Garnett find that 80 percent of microeconomics textbooks misrepresent Coase's arguments. Michael R. Butler and Robert F. Garnett, "Teaching the Coase Theorem: Are We Getting It Right?" *Atlantic Economic Journal* 31 (June 2003): 133–45.

[10] Coase, "Social Cost," 2.

whichever party has the lowest cost of avoiding the reciprocal harm, in fact, avoids it. This creates a severe difficulty for regulatory and Pigovian solutions to externality problems. The regulatory authority may not know which party is the least-cost avoider, and there will naturally be little incentive for this party to step forward and volunteer to adjust its actions.

Under certain conditions, markets will naturally tend to internalize externalities. Stigler dubbed this result the Coase Theorem.[11] In part because the formulation of this theorem was not Coase's primary objective in writing his article, there is no canonical statement of the Coase Theorem. For our purposes, it is enough to say that markets will efficiently cope with externalities when property rights are sufficiently well-defined and transaction costs are sufficiently low.[12]

Consider the externality created by a rancher's cattle wandering into a farmer's field and trampling the crops. Suppose that the initial allocation of rights is such that the rancher bears no liability and that only the rancher has the right to build a fence to contain his cattle. If we suppose that the crop damage is greater than the cost of building a fence and that transaction costs are sufficiently low, then the farmer will pay the rancher to build a fence to contain the cattle. If the rancher bears liability, he will build the fence of his own volition to reduce the liability. If, in contrast, only the farmer has the right to build the fence, the rancher will pay the farmer to build the fence if the rancher bears liability, and the farmer will build it freely if the rancher bears no liability. The fence gets built no matter who bears liability and no matter who has the right to build the fence, as long as the cost of building the fence is less than the damage to

---

[11] Coase is very clear both that the origin of the term is with Stigler and that it was not the main point he was trying to make. Ronald H. Coase, *The Firm, the Market, and the Law* (Chicago: University of Chicago Press, 1988), 14, 157.

[12] Some versions add that the allocation of resources will be invariant to the initial distribution of rights if wealth effects are sufficiently small.

the crops from trampling. If the damage to the crops from trampling is smaller than the cost of building the fence, the fence will not be built, no matter who has liability or the right to build a fence.

"Simple" Coasian internalization is not just theoretical. For 20 years, Meade's example of the external benefits that characterize the interaction of beekeepers and apple farmers was cited as a canonical example of market failure.[13] According to Meade, both the bees' pollination of apple orchards and the orchards' supply of food for bees are unpaid factors. The net externality would be zero only by an astonishing coincidence, and therefore either beekeepers or apple farmers should be subsidized to correct the market failure. It was not until Cheung actually investigated the joint production of honey and apples by talking to beekeepers and farmers that economists realized that no market failure occurs here.[14] In fact, apple farmers, among others, routinely pay beekeepers for pollination services. The payment varies depending on the season and the crop to be pollinated since these factors affect the quality of the bees' honey. In other words, there is a robust market correcting Meade's alleged market failure.

The reciprocal nature of externalities should make one reticent to hastily declare that an externality is a market failure. A visible harm may create benefits that are more difficult to see and larger in magnitude than the harm itself. When that is the case, it is efficient for the harm to persist, whether or not payment is made to compensate for the harm. When property rights are well-defined and transaction costs are low, payment *will* be made if necessary to ensure the efficient outcome. When there is a market solution to an externality problem, parties will have the incentive to efficiently mitigate the harm or increase the benefit. When these efforts are

---

[13] James E. Meade, "External Economies and Diseconomies in a Competitive Situation," *Economic Journal* 62 (March 1952): 54–67.
[14] Steven N. S. Cheung, "The Fable of the Bees: An Economic Investigation," *Journal of Law and Economics* 16 (April 1973): 11–33.

nonobvious, market solutions will strictly dominate regulatory solutions. For our purposes, it is important to recognize that when externalities are efficiently internalized through market arrangements, *the visible external harm or benefit will often persist*. Because the external harm or benefit has already been efficiently internalized, regulatory or Pigovian interventions will make the outcome strictly less efficient. As a result, the identification of a persistent externality is not sufficient for a declaration of market failure.

Complex Coasian Internalization

The previous section made the case for what is frequently called the Coase Theorem, the idea that when property rights are well-defined and transaction costs are sufficiently low, externalities will be efficiently internalized through market transactions. Proponents of government intervention will frequently cede this point but argue that a regulatory or Pigovian solution is nevertheless warranted because transaction costs are, in fact, high. Perhaps hundreds of parties may be involved, each with the incentive to behave opportunistically. Nevertheless, a deeper reading of Coase illuminates his fundamental argument that when transaction costs are high, "an alternative form of economic organisation" can mitigate the inefficiency associated with the uninternalized externality.[15] People, in fact, adopt these alternative forms of organization precisely to economize on transaction costs, which enables externalities to be largely internalized.

Coase argues that the *raison d'être* of a firm is to economize on transaction costs.[16] In principle and in the absence of transaction costs, all of a firm's activity could be conducted by mutually contracting independent producers. What a firm does is reduce the transaction costs

[15] Coase, "Social Cost," 16.
[16] Ronald H. Coase, "The Nature of the Firm," *Economica* 4 (November 1937): 386–405.

associated with production. If N participants are required to supply some product, there are potentially $N(N-1)/2$ bilateral contracts necessary between them, whereas if one of them hires the rest, only $N-1$ contracts are necessary. Furthermore, long-term contracting can remove some of the incentives for opportunistic behavior, further lowering transaction costs. Against these reductions in transaction costs, firms must incur the costs associated with centrally directing resources.

Coase uses the example of lighthouses to explicitly discuss how the expansion of a firm can internalize externalities in production.[17] Prior to Coase's article, lighthouses were considered the quintessential public good; they are cited as far back as Mill, Sidgwick, and Pigou as providing an external benefit for which it is difficult to charge.[18] Ships passing in the night benefit from the presence of lighthouses and are very difficult to toll. Consequently, the argument goes, lighthouses must be subsidized or produced by the state; the transaction costs associated with providing lighthouse services are too high for the market to supply lighthouses.

Examining the historical record, Coase found that, in fact, most lighthouses built in Britain during the seventeenth century were privately constructed. The positive externality generated by lighthouses can be internalized when the lighthouse business is vertically integrated with the harbor business. A harbor that is authorized to collect fees from ships that dock will build a lighthouse so that more ships will dock there, generating higher fees. Even though transaction costs are high between lighthouses and ships, an alternative economic arrangement,

---

[17] Ronald H. Coase, "The Lighthouse in Economics," *Journal of Law and Economics* 17, no. 2 (October 1974): 357–76.

[18] John Stuart Mill, "Principles of Political Economy," in *The Collected Works of John Stuart Mill*, ed. J. M. Robson (1965), 968; Henry Sidgwick, *The Principles of Political Economy* (1901), 406; A. C. Pigou, *Economics of Welfare* (1938), 183–84.

the vertically integrated harbor-plus-lighthouse, internalizes a substantial portion of the externality generated by the lighthouse.

Similarly, firms can internalize externalities in consumption. This argument has no canonical citation but is well-known by economists. Consider the case of the nuisance externality generated by smoking in a bar.[19] Smokers impose an external cost on nonsmokers who dislike cigarette smoke. An increasingly common regulatory approach to this problem is to ban smoking in bars. As Coase would emphasize, these bans represent an external, *reciprocal* cost on smokers; if nonsmokers did not go to bars, there would be no point in instituting the ban.

If transaction costs did not exist, the efficient solution would be to accommodate at each instant whichever group, smokers or nonsmokers, had the highest willingness to pay for its preference to prevail. An auction could be held whenever a customer enters or leaves the premises to determine the new efficient rule regarding smoking. Alternatively, customers could make side payments to each other to modify preexisting property rights in the smoking rule. For instance, if the default rule is that smoking is banned, smokers could pay nonsmokers who are present for the right to smoke; if the default rule is that smoking is allowed, nonsmokers could pay smokers who are present to abstain. There would be no market failure because we have assumed that the conditions for simple Coasian internalization hold.

Because in reality transaction costs between smokers and nonsmokers are high enough to preclude bargaining, simple Coasian internalization does not hold. Nevertheless, a more complex Coasian internalization does occur without government intervention—the externality is largely internalized *by the owner of the bar*. The owner is the residual claimant on the value generated by the property and has the incentive to select the efficient rule for his or her customers. When

---

[19] Lee examines this case. See especially the discussion on page 158 in Dwight R. Lee, "Government v. Coase: The Case of Smoking," *Cato Journal* 11 (Spring/Summer 1991): 151–64.

the right to smoke is highly valued, the owner will allow smoking and be able to charge higher prices than if smoking were banned. When the right to be free of the smoking nuisance is highly valued, the owner will ban smoking and once again be able to charge higher prices than if smoking were allowed. Because the owner has an incentive to respond to customers' preferences, laissez-faire complex Coasian internalization will dominate, at least weakly, the government-imposed ban on smoking. Furthermore, the market is able to supply some bars that allow smoking and some that do not, enhancing efficiency. The market is also able to offer middle-ground policies, such as smoking and nonsmoking sections, that may reflect least-cost avoidance of most of the external harm.

As we have seen, it is not enough to cite the existence of an externality and high transaction costs to declare a market failure. Markets can be thought of as searching for value-maximizing forms of economic organization. When high transaction costs exist, markets will adopt arrangements to economize on transaction costs. These arrangements might not outperform an idealized world in which transaction costs do not exist, but frequently they will be more efficient than regulatory solutions to externality problems. Once again, when externalities are internalized in a complex fashion through firms and other transaction-cost-reducing arrangements, *the visible external harm or benefit will often persist*. We still observe external benefits from lighthouses and, at least in jurisdictions that still allow smoking in bars, we still observe nuisance externalities generated by smokers. But these are not market failures; these are problems that the market has solved despite the high transaction costs that plague the primary actors.

Informal Solutions

When property rights are poorly defined, Coasian solutions are much more difficult. Nevertheless, the observation of an externality and poorly-defined property rights still does not constitute conclusive proof of a market failure. Both theoretical and empirical arguments support this claim.

The theoretical construct most useful for evaluating externalities in the absence of well-defined property rights is game theory. The classic game for describing the use of a commons is the Prisoner's Dilemma. The two players must each decide to cooperate with each other or to defect. The players are both better off if both cooperate than if both defect, but, holding constant the strategy of the other player, each player is better off defecting. Since the choice to cooperate or to defect is simultaneous, it is rational for each player to defect, even though this results in an outcome that is strictly worse than if they could both agree to cooperate.

However, the game's dynamics change if the Prisoner's Dilemma is indefinitely repeated. Each individual Prisoner's Dilemma then becomes a subgame in a larger supergame. Instead of the players choosing strategies of "cooperate" or "defect," the players choose *under what conditions* they will cooperate or defect. Information unfolds throughout the supergame, and players' strategies must incorporate how they respond to the information as it arrives. The selection of a good strategy by one or more players can result in a surprising amount of cooperation.

One strategy available to a player is to cooperate as long as the other player cooperates; if the other player ever defects, even once, the first player can inflict punishment by defecting forever (as long as the indefinitely repeated game lasts). This strategy is known in the literature as a "grim trigger." While the grim trigger is theoretically effective, it is so unforgiving that it

performs poorly in some real-world contexts. A more effective strategy is known in the literature as "tit for tat."[20] Under this strategy, a player cooperates if the other player was cooperative in the last turn and defects otherwise. This tends to generate a lot of cooperation. "Tit for tat" with occasional forgiveness will perform even better in some contexts because it is more robust; it eliminates the possibility that two players, each playing "tit for tat," will end up repeatedly defecting because of an error.

More generally, it can be proved that an indefinitely repeated Prisoner's Dilemma game has an *infinity* of equilibria, not just the one uncooperative equilibrium found in the one-shot game. This fact is known as the Folk Theorem, so called because no one knows who originally proved it. The lesson of the Folk Theorem is that context matters. In order to understand if internalization is occurring in the absence of property rights and government intervention, we must carefully study the informal institutions that influence the outcomes.

Elinor Ostrom won the 2009 Nobel Prize in economics for her contributions in this regard. As co-director of the Workshop in Political Theory and Policy Analysis at Indiana University, she led a decades-long research program that evaluated informal institutions in a number of common-pool resource settings. In *Governing the Commons*, Ostrom summarizes some of the findings from settings such as irrigation communities and forest and fisheries management.[21] She finds that some informal institutions for preserving the commons (that is, internalizing externalities) work quite well and others work poorly. Among other features, good institutions tend to have effective monitoring, graduated sanctions, conflict-resolution mechanisms, and at least some degree of noninterference from external governmental authorities.

---

[20] Robert Axelrod and William D. Hamilton, "The Evolution of Cooperation," *Science* 211, no. 4489 (March 27, 1981): 1390–396.
[21] Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge: Cambridge University Press, 1990).

Ellickson investigates the norms surrounding dispute resolution between neighbors in rural Shasta County, California.[22] Although California has laws that govern cattle trespass, Shasta County residents routinely ignore those laws. Locals prefer to handle disputes in what they consider a neighborly manner. Externalities are internalized because social norms are strongly embedded in the county's longtime residents. Violations of norms are punished first with mild gossip and, if they continue, with punishments as severe as violence against the offending cattle. For the most part, problems are caused only by outsiders who do not share the community's norms; recourse to the law and claims for monetary relief are rare.

Even without formal law or well-defined property rights, people will sometimes internalize externalities through informal institutions and norms. Internalization is most likely when interaction is indefinitely repeated and when other elements of good institutions such as monitoring, graduated sanctions, and conflict-resolution mechanisms are present. In situations where good informal institutions and norms exist, it is important that formal government not disrupt the effectiveness of informal mechanisms unless it is certain that the intervention will internalize externalities more effectively and at lower cost. Once again, we see that the mere observation of an externality does not immediately imply the existence of a market failure or the need for regulatory intervention.

Inframarginal Externalities

When externalities are present and Coasian and informal solutions are not possible, it remains the case that a given externality may not constitute a market failure. In a classic article, Buchanan and Stubblebine introduce several distinctions between different kinds of

[22] Robert Ellickson, *Order without Law: How Neighbors Settle Disputes* (Cambridge, MA: Harvard University Press, 1991).

externalities.[23] One important distinction is between marginal externalities and inframarginal externalities. A marginal externality exists when social costs and benefits do not equal private costs and benefits *at the relevant margin*; an inframarginal externality exists when social costs and benefits *do* equal private costs and benefits at the margin in question but *not at all other margins*. When continuous, marginal changes are possible in the scope of the activity under consideration, inframarginal externalities simply do not cause market failures.[24] At the relevant margin, social costs and benefits equal private costs and benefits, so there is no trade, even in principle, that can make at least one party better off and no party worse off.

The case of an inframarginal externality can be illustrated graphically. Figure 1 shows the market for some good that exhibits a positive external benefit. For simplicity, the good is assumed to be produced at constant marginal cost (MC). The private benefits to the consumption of the good are represented in the marginal private benefits (MPB) curve, and the external benefits are represented in the marginal external benefits (MEB) curve. The marginal social benefits (MSB) curve is simply the vertical summation of the MPB and MEB curves; it represents the benefits both to the consumer and to the external party of the consumption of the good.

As figure 1 shows, it is a mistake to assume that because a good confers some external benefit, it will *necessarily* be underproduced. The privately optimal consumption of the good will occur where the marginal private benefits (MPB) curve intersects with the marginal cost (MC) curve, that is, at Q*. The *socially* optimal consumption of the good will occur at the same

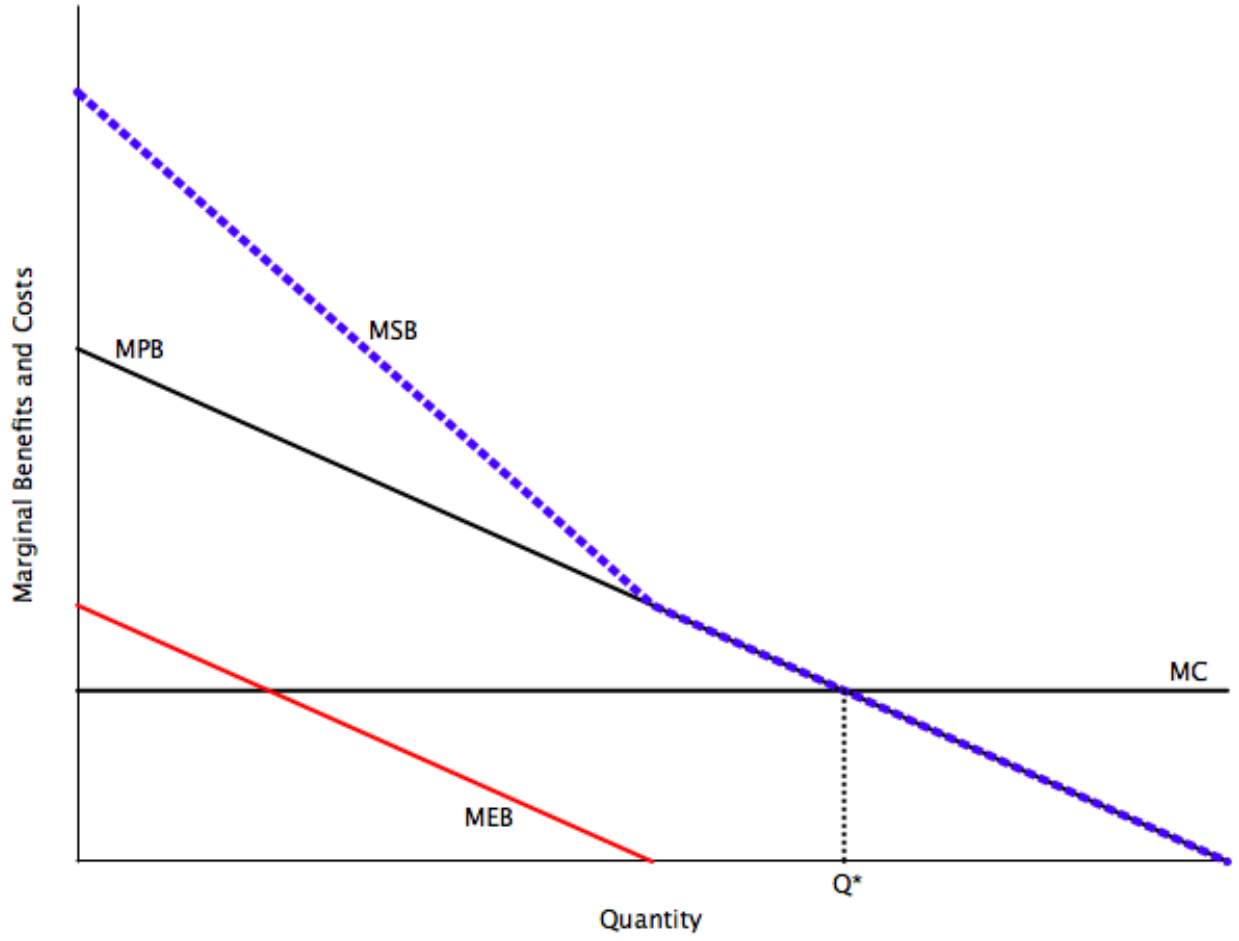
---

[23] James M. Buchanan and William Craig Stubblebine, "Externality," *Economica* 29, no. 116 (November 1962): 371–84. Externalities can be marginal or inframarginal, relevant or irrelevant, and Pareto relevant or Pareto irrelevant. Buchanan and Stubblebine's concept of a Pareto-relevant externality, in the absence of a Coasian or informal solution, constitutes what we have called a market failure.

[24] When only discrete changes are possible in the scope of the activity under consideration, an inframarginal externality will sometimes, but not always, lead to a market failure in the absence of a Coasian or informal solution.

point because the marginal social benefits (MSB) curve intersects the marginal cost (MC) curve at the same point. This is because marginal external benefits are zero at Q*. There is no externality *at the relevant margin*, and therefore no market failure is present.

Figure 1. Market for a good with a positive external benefit



Note: MC=marginal cost; MPB=marginal private benefits; MEB=marginal external benefits; MSB= marginal social benefits.

Again, an inframarginal externality exists when an activity's external costs and benefits occur at relatively high or low levels of the activity, levels that are not under consideration by private actors in the absence of government intervention. An illustration from the market for

education may be instructive, though it should be stressed that the illustration is highly stylized and not meant as an application to education policy. Suppose that it is argued that education confers external benefits; all of society is made better off, it is claimed, if everyone learns how to read and do basic arithmetic. Consequently, education should be subsidized. The conclusion that education should be subsidized follows from the premise that there are externalities associated with basic reading and arithmetic skills only if the margins on which private actors are making educational decisions include the range over which basic reading and arithmetic skills are acquired. Now, arguments have, in fact, been made about positive externalities over the entire range of education, but restricting ourselves to this highly stylized illustration, if such skills are acquired by the sixth grade, and without a subsidy some students will drop out as early as the ninth grade, there is no *market failure* case to be made for a subsidy. A subsidy may increase the total amount of education received, but it will not increase the total amount of external benefits produced in this case.

The logic of inframarginal externalities applies also in more complex cases in which the assumption of zero marginal external benefit or cost does not perfectly hold. Suppose that an activity is characterized by large, even enormous, inframarginal externalities and much smaller marginal externalities. Assuming again that the marginal externalities have not been or cannot be internalized through other means, the market failure created by this structure of externalities justifies at most a small intervention in the market. The enormous inframarginal externalities are simply irrelevant from a market failure perspective if they are not part of the range of outcomes under consideration.

3. The Externalities of Cybersecurity

Having reviewed several arguments for why market failure cannot be immediately inferred from the observation of externalities, this paper now applies these arguments to a number of domains within cybersecurity policy in which some claim that markets have failed and that government intervention is therefore necessary. The domains considered include infrastructure security, botnets and DDoS attacks, and espionage and consumer privacy.

Infrastructure Security

The CSIS argues,[25]

> Exploiting vulnerabilities in cyber infrastructure will be part of any future conflict. If opponents can access a system to steal information, they can also leave something behind that they can trigger in the event of conflict or crisis. Porous information systems have allowed opponents to map our vulnerabilities and plan their attacks. Depriving Americans of electricity, communications, and financial services may not be enough to provide the margin of victory in a conflict, but it could damage our ability to respond and our will to resist. We should expect that exploiting vulnerabilities in cyber infrastructure will be part of any future conflict.

The fact that "cyber infrastructure" is a potential target in a future conflict is not itself an externality or a market failure. It does imply that an efficient level of care ought to be taken to secure these resources. Some of the resources are, naturally, owned by the government. There can be no market failure in terms of these resources because they are not cared for on the market. The level of care taken in securing these resources is a matter of internal government policy, not

[25] CSIS, *Securing Cyberspace*, 13.

informed by the price system or by profit feedback mechanisms; let us hope they get it right. But 85 percent of the critical infrastructure in the United States is owned by the private sector.[26] The important question, therefore, is whether the private sector will undertake the efficient level of care in securing resources whose integrity affects us all.

If the CSIS's claims about the nature of "cyber war" are correct, then there is a clear externality in the provision of security for the resources in question. We all receive an external benefit—a decreased risk of significant disruption—when, say, financial institutions take security precautions. Van Eeten and Bauer argue that such externalities are market failures,[27]

> Many instances of what could be conceived as security failures are, in fact, the outcome of rational economic decisions, based on the private costs and benefits of security as perceived by the actors during the timeframe considered in those decisions. As security is costly, rational players will accept a certain level of security breaches. However, there is an additional aspect to the security issue. If the incentives of the players in the value net do not properly reflect the *social* costs and benefits of their security decisions, for example, because of externalities or public good aspects of security investments, such privately rational decisions will systematically deviate from the social optimum.

However, van Eeten and Bauer do not consider the extent to which infrastructure security externalities are inframarginal and therefore irrelevant from a market failure perspective. In the event of a significant disruption, the firms in question would lose enormous amounts of money and physical capital; they have a strong incentive to take precautions against such an event. Once

---

[26] Deloitte Touche Tohmatsu, *2004 Global Security Survey* (n.p.: Deloitte Touche Tohmatsu, 2004), http://www.deloitte.com/assets/Dcom-Argentina/Local%20Assets/Documents/global_security.pdf.
[27] Van Eeten and Bauer, "Emerging Threats," 223.

firms have exhausted their privately rational security measures, how much of the externality remains? Despite the importance of national security, it is not obvious that the *marginal* externality is very large at all. There is clear evidence that firms that own critical infrastructure spend a great deal on security, and there is not clear evidence of the existence of important, socially worthwhile security measures that they are neglecting to take.

Powell examines security spending in the financial services industry.[28] While rightly pointing out that it is impossible to know from mere observation if a given level of security spending is optimal, he notes that survey evidence from 2004 shows that executives highly value security and that 63 percent of firms reported a security budget increase over the prior year. Baker et al. survey 600 information technology and security executives from critical infrastructure enterprises across seven sectors and find that "[e]ven in a recession, security is still the top factor in making IT investment and policy decisions."[29] PricewaterhouseCoopers interviews 12,840 executives and finds that 71 percent of respondents affirm that increasing the focus on data protection is an important priority.[30] Soo Hoo estimates that firms *overinvest* in cybersecurity, finding a lower marginal rate of return on cybersecurity investments than on other technology investments.[31]

---

[28] Benjamin Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry" (Independent Institute Working Paper 57, The Independent Institute, Oakland, CA, 2001), http://www.independent.org/pdf/working_papers/57_cyber.pdf.
[29] Stewart Baker, Shaun Waterman, and George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War* (Santa Clara, CA: McAfee, 2009), 14, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.
[30] PricewaterhouseCoopers, *Respected—But Still Restrained: Findings from the 2011 Global State of Information Security Survey* (n.p.: PricewaterhouseCoopers, 2010), 17, http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf.
[31] Kevin J. Soo Hoo, "How Much Is Enough? A Risk Management Approach to Computer Security" (working paper, Consortium for Research on Information Security and Policy, Stanford, CA, June 2000), http://iis-db.stanford.edu/pubs/11900/soohoo.pdf.

What stands out about the concerns over infrastructure security is a relative paucity of specific examples of precautions that firms are failing to implement. The incentive to protect the firm's assets is enough to ensure the implementation of commonsense practices such as updating server software and installing virus detection programs. If firms that own critical infrastructure underinvest in security, it seems probable that the binding limitation is not so much the incentive to invest, but ignorance about what additional cost-effective precautions they could take. This is not a trivial problem. Hypothetically, if a regulatory agency were to mandate certain security practices that are not widespread today, what welfare-improving practices would they mandate? To the extent that *we just do not know* what else to do to improve infrastructure security, the positive externality associated with security is irrelevant from a market failure perspective. Those who are concerned about infrastructure security could improve welfare by producing evidence that particular security precautions that are not widely deployed today are cost-effective.

While unregulated private firms have a strong incentive to protect their capital, regulated public utilities present a more difficult case. It is at best unclear whether these firms will invest in sufficient security procedures and precautions. If one regards the provision of network security as a form of capital maintenance, then one can draw on a substantial literature on rate-of-return regulated monopolies. Ronen and Srinidhi find that capital maintenance and purchase decisions for rate-of-return regulated monopolies will depend upon the specific accounting rules for depreciation, something that would be irrational for a private firm competing on the market.[32] Westfield shows that rate-of-return regulated monopolists can earn higher profits if their

[32] Joshua Ronen and Bin Srinidhi, "Depreciation Policies in Regulated Companies: Which Policies Are the Most Efficient?" *Management Science* 35 (May 1989): 515–26.

suppliers collude to raise prices.[33] Sherman shows how capital waste can be motivated even when the marginal product of capital is positive.[34] Since the investment behavior of rate-of-return regulated monopolies can depend on the specific regulations they face, a complete treatment of their investment in security procedures is beyond the scope of this paper. Nevertheless, it is at minimum clearly possible that public utilities underinvest in security in a sense that is irrelevant to unregulated firms. If upon inspection it seems that these firms do underinvest in security, this should be considered a government failure, not a market failure; despite the nominally private status of these firms, they are creatures of the state, not of the market.[35]

As this paper has argued, inferring a market failure is a subtle, tricky task. My claim is not that there is definitively no market failure with respect to unregulated firms in the market for critical infrastructure, but that the available evidence of a market failure is weak. If there is a market failure, it is surely much smaller than a naïve application of popular but misguided principles of public economics would suggest. There is also a serious danger of government failure. What would a Pigovian or regulatory solution to this externality problem look like? Pigovian logic would prescribe a subsidy, perhaps a "security spending tax credit," to attempt to adjust for the external component of security spending. Such a subsidy would be unlikely to result in substantially greater security; rather, existing staff would be nominally reclassified as "security personnel" and firms would use accounting tricks to expand their apparent security budgets. Some of the increased spending could increase actual security, but at a price that is not

---

[33] Fred M. Westfield, "Regulation and Conspiracy," American Economic Review 55, no. 3 (June 1965): 424–44.
[34] Roger Sherman, "Capital Waste in the Rate-of-Return Regulated Firm," Journal of Regulatory Economics 4 (1992): 197–204.
[35] The possibility of insecurity generated by public utilities strengthens the case for laissez-faire over the textbook analysis of natural monopolies. Governments should search for market modes of provision for critical infrastructure, even when this results in a price that is higher than marginal cost; cybersecurity alarmists should presumably welcome greater security at the expense of higher prices of service.

even *socially* cost-effective. A regulatory mandate might fare no better. If it is not obvious what socially efficient practices private firms are neglecting to take, it is difficult to require firms to implement them. Requiring firms to implement practices that turn out not to be socially cost-effective is obviously inefficient.

Botnets and DDoS Attacks

Van Eeten and Bauer (2009) argue that the externalities associated with botnets constitute a market failure that requires collective action.[36] Modern malware (malicious software) coders have written viruses that enable them to control infected machines and use a network of them, called a botnet, to send spam or participate in distributed denial of service (DDoS) attacks. In a DDoS attack, the botnet "herder" directs thousands of infected machines to send massive amounts of traffic to particular servers, making it hard for those servers to respond to legitimate requests while the attack is ongoing.

> We find that the incentives under which end users and ISPs operate explain the emergence of botnets and thus generate information security problems for society at large. A large part of these problems constitutes an 'externality', a cost imposed on stakeholders by the actions of other stakeholders, for which they have no recourse to compensation.[37]

The proximate source of the problem is end users: "In sum, end users in the aggregate spend too little on security; their decisions therefore enable the growth of botnets, which impose costs on virtually every other actor in the network."[38]

---

[36] Van Eeten and Bauer, "Emerging Threats."
[37] Ibid., 223.
[38] Ibid., 224.

The incentives of Internet service providers (ISPs) to control malware are limited. Van Eeten and Bauer cite the U.K. House of Lords Science and Technology Committee, which reports:

> At the moment, although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so. Indeed, there is a disincentive, since customers, once disconnected, are likely to call help-lines and take up the time of call-centre staff, imposing additional costs on the ISP.[39]

They also note that more recently, ISPs have increased their efforts against malware. Since van Eeten and Bauer's article was published, Comcast, one of the largest ISPs in the United States, began a proactive bot notification service.[40]

At one level, the case of computer viruses is remarkably similar to that of smoking in bars discussed in the previous section. On a given ISP, some customers are infected and some are not. The ISP faces a choice to restrict access by the infected machines or to let them continue to inflict some modest harm on other users in the form of congesting the network and raising the risk of infecting other machines. These modest harms are clearly internalized by the ISP in its choice of policies and prices. The ISP could offer a different bundle of service conditions and prices, but it offers instead the most profitable one, which is the one that creates the most value. For instance, the ISP could shut down access for all infected users, raising support costs. To cope with support costs, it could raise prices to all users or charge per support incident. ISPs *must* believe that consumers prefer the status quo arrangement instead. As with smoking in bars, to the

---

[39] U.K. House of Lords, Science and Technology Committee, *5th Report of Session 2006–07, Personal Internet Security, Volume I: Report* (London: House of Lords, August 10, 2007), 30, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf, cited in van Eeten and Bauer, "Emerging Threats."

[40] For details, see Comcast Interactive Media, "Constant Guard New Update," 2011, http://security.comcast.net/constantguard/.

extent that ISPs allow infected users to continue using their networks, it appears to be socially efficient for uninfected users to tolerate infected users.

What about externalities between ISPs? Van Eeten and Bauer document the robust informal networks that align ISPs' interests:

> An incentive that was mentioned by all interviewees is related to the informal networks of trusted security personnel across ISPs, CSIRTS [Computer Security Incident Response Teams] and related organizations…. When describing how their organization responded to security incidents, interviewees would refer to personal contacts within this trust network that enabled them, for example, to get another ISP to quickly act on a case of abuse. These contacts are reciprocal. They are also contacted about abuse in their own network and are expected to act on that information.[41]

These informal connections appear to provide necessary enforcement of norms at low social cost:

> As one interviewee explained: 'What enforces security on a service provider is threats from other service providers'. One ISP security officer told us that the informal contacts imply cost savings. Less staff time is needed to deal with the fallout of a security incident—e.g., going through time-consuming procedures to get off blacklists—and to deal with customer support.[42]

It appears that these informal norms are capable of relatively efficiently internalizing the externalities that exist *between ISPs* with respect to botnets. The informal networks consist of indefinitely repeated interactions, monitoring, graduated sanctions, and so on, as Ostrom

---

[41] Van Eeten and Bauer, "Emerging Threats," 227.
[42] Ibid.

suggests would be necessary for maintaining a common pool resource without outside enforcement.[43]

There does not appear to be a substantial market failure between end users on a single ISP or between ISPs; what about between the infected users and the operators and users of DDoS targets? It is possible that the least-cost avoiders of the externality in this case are the operators of DDoS targets themselves. As van Eeten and Bauer report, one Georgian newspaper, faced with a DDoS attack emanating out of Russia during the 2008 invasion, moved its operation to Blogger, which is hosted on Google's robust infrastructure.[44] The point is not that newspapers should be hosted on Blogger; rather, a cheap and effective way to protect against DDoS attacks is to host one's site on a large, shared grid. Combined with modern techniques such as edge caching, this solution seems to substantially eliminate the problems associated with DDoS attacks at a cost much lower than, say, training users not to get infected.[45]

Lichtman and Posner advocate indirect liability for ISPs for the damage caused by botnets and other malware, arguing that the case for indirect liability is bolstered when transaction costs are high:[46]

> Conventional economic analysis suggests that an explicit rule imposing indirect liability is not necessary when two conditions are simultaneously met: first, the relevant direct actors are subject to the effective reach of the law, by which we mean that the employees, drivers, and merchants discussed in our previous

---

[43] Ostrom, *Governing the Commons*.
[44] Van Eeten and Bauer, "Emerging Threats."
[45] It is also not clear that the stability of the websites that are frequently targets of DDoS attacks should be such a high priority. The popular comic strip XKCD recently alluded to this in a strip, "CIA," in which a news reporter announces, "Hackers briefly took down the website of the CIA yesterday…" According to the author, people hear: "Someone hacked into the computers of the CIA!!" Computer experts hear: "Someone tore down a poster hung up by the CIA!!" Randall Munroe, "CIA," comic strip, XKCD blog, August 1, 2011, http://xkcd.com/932/.
[46] Doug Lichtman and Eric Posner, "Holding Internet Service Providers Accountable," *Supreme Court Economic Review* 14 (2006): 229.

> examples are easy to identify and have assets that are sufficient to pay for any harm caused; and, second, transaction costs are such that those direct actors can use contract law to shift responsibility to any party that might otherwise be an attractive target for indirect liability. The intuition is that, when these conditions are satisfied, the various parties can create indirect liability by contract, and—albeit subject to some second-order constraints—will do so where that would be efficient.

They proceed to argue that because transaction costs are high between actors on the Internet, ISPs should not continue to be exempt from indirect liability by congressional statute. Lichtman and Posner carefully consider whether the network of peering contracts between ISPs could provide a basis by which ISPs could allocate liability efficiently. After all, if firms are contracting anyway, then at the margin transaction costs are very low. They conclude that ISPs could not efficiently allocate liability:

> [A]ny network of contracts focusing on issues of cyber-security would be perpetually out of date, and updating such a complicated web of interdependent security obligations would be all but impossible given the number of parties involved and the complicated questions any update would raise regarding the appropriate adjustments to the flow of payments.[47]

However, this analysis ignores the possibility of informal enforcement of liability norms between ISPs. As this paper has argued, ISPs rely on informal interactions to align their interests and to enforce good security practices on other ISPs. This informal system *functions as an alternative legal system*. It should not be inferred that because it is less formal than the legal

[47] Ibid., 235–36.

system Lichtman and Posner have in view, it is inferior; on the contrary, precisely because the informal network of relationships does not require written contracts, it is more flexible and can more effectively deal with the dynamic nature of threats to network security. The danger is that Lichtman and Posner's proposed solution of indirect liability could result in the breakdown of the informal network that now internalizes externalities; firms that now cooperate could be placed at odds with each other. This extremely cost-effective method of dispute resolution would be replaced with more costly adventures in the U.S. court system. Consequently, it seems likely that indirect liability for ISPs would reduce, not enhance, economic efficiency.

Rather than representing a case of market failure, botnets and DDoS attacks appear to represent a case of the market coping with externalities in a relatively efficient way. As with infrastructure security, the risk of government failure is acute. If ISPs are required to shut down access from all infected computers even when the externalities are largely internalized, it will increase support costs, and therefore the cost of Internet access, unnecessarily. To the extent that this does not represent least-cost avoidance, such a regulation would decrease, not increase, social welfare. Assigning indirect liability to ISPs for the damage caused by botnets and other malware would weaken the informal networks that now resolve disputes between ISPs. This, too, could have significant welfare costs because it would raise the cost of dispute resolution between ISPs.

Espionage and Consumer Privacy

Different countries have adopted different rules with respect to consumer privacy. One concern is that since consumers cannot directly observe the security practices of the firms with which they are dealing, the firms will shirk their security duties. In response to this concern, the

EU has enacted strict regulations regarding data privacy and protection, beginning with the Data Protection Directive in 1998 and the Directive on Privacy and Electronic Communications in 2003. The *New York Times* reported that the EU is considering extending its data breach notification rules from phone service and Internet access to online banking, video games, shopping, and social media.[48] Mandatory notification of breaches reduces the shirking externality by making the firm pay a cost in reputation when a breach occurs.

Despite the apparently modest nature of this regulation, it is not clear that a substantial market failure exists in the realm of data breaches. Service providers offer terms of service to their customers.[49] These terms can include a provision that requires notification of any data breach, which can be enforceable in court. Indeed, the U.S. Department of Commerce operates a program called Safe Harbor that allows American companies to affirm that they abide by the standards of the EU's Data Privacy Directive.[50] This voluntary program, while directed toward companies that export services to the EU, is open to any U.S. firm; familiar companies such as Google and Facebook tout their compliance in their privacy policies. [51] There are private certifications as well; Payment Card Industry (PCI) requires that firms that process credit card payments adhere to its data security standards, which include breach notifications.[52] If consumers value data breach notifications or any other security services, they can patronize companies that promise to deliver them (and pay, either through user fees or exposure to advertisements, for the

---

[48] James Kanter, "Europe Leads in Pushing for Privacy of User Data," *New York Times*, May 3, 2011, http://www.nytimes.com/2011/05/04/technology/04iht-privacy04.html.
[49] For instance, Facebook's privacy policy is located at https://www.facebook.com/about/privacy/.
[50] A list of firms that so affirm is available at https://safeharbor.export.gov/list.aspx.
[51] Google, "Privacy Policy," October 20, 2011, http://www.google.com/privacy/privacy-policy.html; Facebook, "Data Use Policy," September 23, 2011, https://www.facebook.com/full_data_use_policy.
[52] PCI's security standards are available at https://www.pcisecuritystandards.org/security_standards/.

cost of reducing breaches).[53] Yet not all services require the disclosure of sensitive information, and some consumers may use services in ways that do not expose sensitive information. In these cases, the regulation imposes an unnecessary burden on service users, who ultimately pay for more security than they wish to purchase.

One virtue of the market is that it can accommodate differing preferences with regard to safety. We do not and should not require that all cars be as safe as technologically possible. Relatively unsafe cars are part of the optimal stock of cars. Similarly, relatively insecure online services are part of the optimal stock of online services. In the presence of easily accessible online terms of service that can include a notification provision, mandatory notification of data breaches seems likely to oversupply security services.

Finally, it seems clear that firms are sensitive to the effects that breaches of data privacy have on their reputations and bottom lines. For instance, the April 2011 breach of Sony's PlayStation Network was a major embarrassment to the firm. In response, the company offered $1 million of identity theft insurance to every user of the network.[54] Sony faces multiple lawsuits related to the incident.[55] Firms can also gain from being good stewards of customer privacy. In 2006, privacy advocates praised Google for resisting a U.S. Department of Justice subpoena on pornographic search terms.[56] Google succeeded in substantially limiting the subpoena's scope.

---

[53] Some commentators might argue that the problem is that consumers do not value privacy and data security enough, and that therefore these things are underprovided. This is ultimately a claim about what constitutes the right value system. Conventional economic analysis respects subjective values, so it would ascribe low importance to privacy if consumers place a low value on it. The decision to respect subjective preferences is itself a normative one, but it is nevertheless standard procedure in public economics; consequently, it is the approach that I follow.

[54] Sony CEO Howard Stringer's letter to users is available at http://blog.us.playstation.com/2011/05/05/a-letter-from-howard-stringer/.

[55] Erica Ogg, "Sony sued for PlayStation Network data breach," *CNET*, April 27, 2011, http://news.cnet.com/8301-31021_3-20057921-260.html; Mike Rose, "Canadian Law Firm Files $1B Lawsuit Against Sony Over PSN Data Breach," *Gamasutra*, May 4, 2011, http://www.gamasutra.com/view/news/34499/.

[56] Katie Hafner and Matt Richtel, "Google Resists U.S. Subpoena of Search Data," *New York Times*, January 20, 2006, http://www.nytimes.com/2006/01/20/technology/20google.html.

The firm's concern for its reputation and bottom line represents the Coase Theorem in action; a substantial portion of any data privacy externality is internalized by the market.

Again, it is difficult to see how there could be a substantial market failure in terms of data privacy if firms can announce in advance how they will protect customer data and if they will notify customers of any breaches. Customers can patronize companies that announce acceptable policies. Although the proposed regulations have been relatively modest, they might nevertheless lower welfare and result in government failure. They are likely to oversupply security services; the portion of the additional cost that exceeds the value that consumers place on the added security is a welfare cost. The additional cost will raise the price of services (or, in the case of free services, the equilibrium amount of advertising) and therefore discourage some users from consuming the product. Finally, high regulatory burdens disproportionately harm small businesses and startups. Well-capitalized companies can easily comply with security regulations, but a new online service may not have the resources to carefully parse and implement the legal requirements. Consequently, unnecessary regulations can have the unintended effect of making the economy less dynamic by discouraging startups and small firms.

Conclusion

Market failure is a more complex topic than many policy analysts realize. As this paper has argued, it does not immediately follow that an externality, without government intervention, will lead to a market failure. Market failure needs to be carefully inferred, not gleefully declared at the first sight of deviations from a perfect competition model. Cybersecurity policy provides an interesting set of cases in which, after investigation, the market failure is much smaller than it appears at first glance, if it exists at all.

Policy makers should be careful not to interfere with economic activity unless there is clear evidence of market failure. Inappropriate regulation, whether it is too stringent or just misapplied, can lead to large welfare costs that are as significant and as real as those that result from market failure. The risk of "government failure" is often overlooked by policy analysts, but it is severe. Consequently, the burden of proof should be on those who wish to intervene in the Internet economy to provide (1) clear evidence of the existence of actual market failure, not just observable externalities, and (2) a regulatory solution that is likely to do more good than harm. These are substantial burdens that do not appear to have been met.