2007

Property Rules, Liability Rules, and Immunity: An Application to Cyberspace

Keith Hylton
Boston Univeristy School of Law

PROPERTY RULES, LIABILITY RULES, AND IMMUNITY:
AN APPLICATION TO CYBERSPACE

KEITH N. HYLTON

Property Rules, Liability Rules, and Immunity:

An Application to Cyberspace

Keith N. Hylton*

(May 2006)

Abstract: This paper sets out a theory of torts and cyberspace wrongs. Its goal is to set out a sparse theoretical account of tort law and apply it to cyberspace torts, both negligent and intentional. I approach this goal by applying the framework of property rules and liability rules to cyberspace torts. That framework suggests that trespass doctrine is appropriate in instances of cyber-invasions of private information resources, such as the breaking of codes to access private information on the web. However, trespass doctrine should play no role in cyber-invasions of public information resources, such as the sending of spam email. I also examine indirect liability claims against operating system sellers or internet service providers for the harms caused by cyberspace actors (e.g., virus writers, copyright violators). The theory presented here suggests that the basis for strict indirect liability is weak. Finally, the theory suggests that immunity rules should play a role in this area, though in a smaller set of instances than those protected by the Communications Decency Act.

* Professor of Law, Boston University, knhylton@bu.edu. For helpful comments I thank workshop participants at Copenhagen Business School, especially Henrik Lando. I thank Nicola Leiter and Dena Milligan for research assistance. This research was supported by Boston University and Microsoft. The views expressed, as well as errors and omissions, are entirely my own.

I. Introduction

Legislative proposals to usher in an era of "electronic medicine" have helped identify as a puzzle the failure of the medical industry to keep up with information technology.[1] Many have noted that financial records and credit histories are contained in electronic libraries, while medical records are still stored in manila folders.[2] Perhaps one reason for this is the number of things that can go wrong with information technology or, more simply, software.

Consider just a few examples of the things that could go wrong with software in the medical industry. Suppose a company introduces a cardiac defibrillator (a machine that emits an electric jolt to correct an irregular heartbeat) that is surgically inserted into the patient's body and uses a software program to govern itself as well as allow physicians to monitor its activity. Suppose a defect in the software causes the electric impulses to fire at the wrong times or fail to fire at the right times.

As a second example, suppose medical patient records are stored in an electronic library. A hacker gets access to the library and alters records. Third, suppose a hacker releases a "spider" that crawls through medical records and forwards the information to others or makes it publicly available. Or, returning to the defibrillator example, suppose the hacker finds a way to control the functioning of the defibrillator. It is easy to see that the harms that might result from defective or insecure software in the medical setting could be orders of magnitude greater than those observed in the more common settings

[1] For an example of a recent legislative proposal to introduce electronic medicine, see Statements & Releases, New York Senator Hillary Rodham Clinton, Frist, Clinton Introduce Health Technology to Enhance Quality Act (June 16, 2005), http://www.senate.gov/~clinton/news/statements/details.cfm?id=239875.

[2] See, e.g., IT in the Health Care Industry, ECONOMIST, April 30, 2005, at 65.

involving financial records. Fear of the potential harm and resultant liability could be a major reason technology companies have not rushed in to the electronic medicine market.

Electronic medicine is just one of many examples in ordinary life in which software flaws can lead to serious harms, and liability for those harms. We already have examples of computer viruses that have caused enormous damage to property and to commercial transactions.[3] And each of us by now is familiar with the problem of "spam" electronic mail and the burdens it imposes.

This paper attempts to set out a general theory of torts and cyberspace wrongs. It differs from the previous literature in this area by avoiding the piecemeal approach taken in most articles.[4] The goal here is to start with a theoretical account of tort law and to apply that to cyberspace torts, both negligent and intentional. I approach this goal by applying the framework of property rules and liability rules to cyberspace torts. That framework suggests that trespass doctrine is appropriate in instances of cyber-invasions of private information resources, such as the breaking of codes to access private information on the web. However, trespass doctrine should play no role in instances of

[3] See, Robert W. Hahn and Ann Layne-Farrar, The Law and Economics of Software Security, draft on file with author, pp.15-20 (detailing costs of software security breaches), 2006.

[4] I do not intend the description "piecemeal" as pejorative. I am simply referring to the tendency in the literature to focus on one particular type of cyberspace tort theory, such as trespass or nuisance. For examples of excellent articles that are in the piecemeal tradition, see Adam Mossoff, Spam – Oy, What a Nuisance!, 19 Berkeley Tech. L. J. 625 (2004); Richard A. Epstein, Cybertrespass, 70 U. Chi. L. Rev. 73 (2003). There are articles that have taken a more general approach to determining the appropriate legal regime. Most of these articles focus on the appropriate analogy or metaphor for thinking about torts in cyberspace. See, e.g., Dan L. Burk, The Trouble With Trespass, 4 J. Small & Emerging Bus. L. 27 (2000); Dan Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 Calif. L. Rev. 439 (2003); Mark A. Lemley, Place and Cyberspace, 91 Calif. L. Rev. 521 (2003); Richard A. Epstein, Intel v. Hamidi, The Role of Self-Help in Cyberspace?, 1 J. Law Econ. & Policy 147 (2005); David McGowan, The Trespass Trouble and the Metaphor Muddle, 1 J. L. Econ. & Policy 109 (2005); Maureen O'Rourke, Property Rights and Competition on the Internet: In Search of an Appropriate Analogy, 16 Berkeley Tech. L. J. 561 (2001); Jonathan J. Rusch, Cyberspace and the "Devil's Hatband", 24 Seattle U. L. Rev. 577 (2001); Alfred C. Yen, Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace, 17 Berkeley Tech. L. J. 1207 (2002). See generally, Symposium: Property Rights on the Frontier: The Economics of Self-Help and Self-Defense in Cyberspace, J. Law, Economics & Policy, volume 1, Winter 2005. The present paper differs from this literature in the sense that it sets up a general framework for tort law and shows that it applies to cyberspace wrongs.

cyber-invasions of public information resources, such as the sending of spam email. Another set of cases I examine are those in which plaintiffs assert indirect liability claims against operating system sellers, internet service providers, or software developers for the harms caused by some cyberspace actors (e.g., virus writers, copyright violators). The theory presented here suggests that the basis for strict indirect liability is weak. Finally, the theory suggests that immunity rules should play a role in this area, though in a much smaller set of instances than in existing law.

II. A Few Examples

To get a clearer sense of the problems that arise in this area, I will start by describing a few of the better known cases in the intersection of torts and cyberspace. Of course, information technology is constantly evolving, so a description of previous cases may not tell us much about the problems that will arise in the future. Still, the previous cases have set out several issues that courts are still grappling with in their efforts to apply tort law to a new realm.

In *Blumenthal v. Drudge*,[5] Matt Drudge reported in his column disseminated by America Online that Clinton White House aide Sidney Blumenthal had physically abused his wife in the past. Blumenthal filed a defamation suit against Drudge and America Online. At the time of the suit, America Online paid Drudge $3,000 per month to write the column, and exercised certain editorial rights over the column's content, including the right to demand changes and to remove it.[6] Still, the court found that America Online

[5] 992 F. Supp. 44 (D.C. Cir. 1998)
[6] Id. at 51.

was entitled to immunity under Section 230 of the Communications Decency Act.[7] The trial judge noted that if he were "writing on a clean slate",[8] he would have held America Online liable in accordance with the legal standards applied to ordinary publishers.

In *Intel Corp. v. Hamidi*,[9] the plaintiff Intel Corporation maintained an electronic mail system accessible by the internet. A former employee of Intel sent thousands of emails (up to 35,000 at a time) criticizing the company's employment practices to Intel employees.[10] Intel filed suit, claiming that the emails distributed without the company's consent constituted trespass to chattels. Reversing an injunction issued by the lower court, the California Supreme Court held that in order to prevail on a trespass-to-chattels theory the plaintiff had to prove some actual injury resulting from the defendant's conduct.[11] Intel had not presented evidence of an actual injury to the functioning of their electronic mail system.

The third and last example needs no specific legal case, and there have been no reported cases litigated to judgment involving civil liability.[12] Consider a virus disseminated by electronic mail that injures thousands of computer users by destroying files or damaging hard drives. In every such instance there is usually some step that an operating system seller or internet service provider could have taken to prevent the spread of the virus. Some commentators have argued that operating system sellers should be held strictly liable for viruses, since the expected liability would cause the price of the

[7] Id. at 52-53.
[8] Id. at 51.
[9] 71 P.3d 296 (Cal. 2003).
[10] Id. at 301.
[11] Id. at 306.
[12] One claim for damages was filed by a victim of identity theft in 2003, Steve Lohr, Product Liability Lawsuits are New Threat to Microsoft, N.Y. Times, October 6, 2003, at C2. There have been criminal prosecutions, see Victor Homola, World Briefing Europe: Germany: Sasser Hacker is Sentenced, N. Y. Times, July 9, 2005, at A2.

relatively insecure operating system to rise in comparison to the relatively secure system.[13] However, strict liability is not the rule, and there have been no reported cases of third-party (or indirect) liability for viruses.

Although there are many other examples of torts in cyberspace,[14] the examples just given present three general issues with which courts have only begun to grapple. The first, represented by the *Blumenthal* case, is whether internet service providers (or, more generally, others connected to the internet) should be immune for defamation and other information-based torts (e.g., intentional infliction of emotional distress) because the societal benefits of free communication are so great relative to the isolated harms resulting from the relatively infrequent intentional tort. The second issue, represented by *Hamidi*, is whether the rules of trespass, nuisance, or negligence should apply to torts in cyberspace.[15] In terms familiar to legal academics, the question is whether "property rules" or "liability rules" should apply to cyberspace torts. The third issue, represented by the virus example, concerns the choice among liability rules – should they be based on strict liability or negligence principles?

The underlying premise of this paper is that the theories reflected in tort doctrine are general and ought to apply without any serious modifications to cyberspace torts. There is no need for a special field of cybertort law. However, because cyberspace torts are novel, they provide lawyers an opportunity to gain a deeper appreciation and understanding of the rules that they have studied for so long.

---

[13] Douglas Lichtman, Holding Internet Service Providers Accountable, Regulation, Winter 2004-2005, 54-59; Douglas Lichtman and Eric A. Posner, Holding Internet Service Providers Accountable, 14 Supreme Court Economic Review 221 (2006).

[14] See, e.g., Robert W. Hahn and Ann Layne-Farrar, supra note 3, at 6 (describing several categories of cyber-attack: denial of service, viruses (or worms), phishes, spyware, trojan horses, and program back doors).

[15] Richard A. Epstein, Cybertrespass 70 U. Chi. L. Rev. 73 (2003).

III. General Issues

As the examples discussed in the previous section suggest, there are three general issues raised by cyberspace torts. The first is whether and specifically where *property rules* or *liability rules* should apply in this area of torts.[16] Property rules are exemplified by trespass doctrine. A property rule, such as trespass, permits the party protected by the rule to enjoin the injuring party and to collect damages for any violations that occur.[17] Property rule protection forces the potential injurer or invader to bargain with the protected party in order to gain access to the protected party's property. In order to gain access under the property rule, the invader will have to meet the demand price of the protected party, which will be set high enough to cover the protected party for all the injuries that party perceives to be associated with giving access to the invader. If, for example, the invader is incapable of doing any harm to the protected party's property, but the protected party still wants to be compensated for the mere thought that someone else will have access to his property, that perceived harm will be part of the demand price the protected party communicates to the potential invader.

Liability rules, in contrast, do not permit the protected party to enjoin the injuring party. For example, a negligence lawsuit brought against a careless driver is an instance in which a victim asserts liability rule protection. There is no background assumption that the careless driver should have obtained permission from the victim to impose the

[16] On property and liability rules generally, see Guido Calabresi and Douglas Melamed, Property Rules, Liability Rules and Inalienability: One View of the Cathedral, 85 Harv. L. Rev. 1089 (1972).
[17] Id. at 1092.

risk of an injury. The liability rule seeks simply to reallocate to the injurer some objective estimate of the victim's loss after it has occurred.

The second general issue raised by cyberspace torts is, assuming liability rules apply, what type of liability rule should apply and specifically where? Tort law provides two general types of liability rule: strict liability and negligence. The key difference between the two is that under negligence, courts inquire into the care that the injurer took in his conduct, while under strict liability there is no inquiry into the injurer's level of care. Strict liability sounds like "absolute liability", in the sense of imposing liability simply for acting. But there are few if any examples of absolute liability in the law. Most cases of strict liability involve some point at which the injurer made a choice to impose harms on the victim; for example, by choosing to locate his smoke-belching factory next door to the victim's house. And it is this choice that the law aims to control through strict liability.

The third general issue raised by cyberspace torts is whether there should be any liability at all. The issue is actually more complicated. Perhaps the better way to state the issue is the degree to which some liability rule weaker or more lenient than negligence should apply. "Weak negligence" rules would couple the negligence rule's general inquiry into fault with a set of broad defenses that would often permit the injurer to avoid liability altogether. Should there be absolute immunity or "weak negligence" in the field of cyberspace, and specifically where should immunity or weak negligence rules apply?

I take up each of these issues in the following section, though I will focus on torts generally. I will synthesize existing theories and extend them in order to provide a

framework that explains the overall shape as well as the details of tort law. After setting out a positive framework, I will apply it to cyberspace torts.

A. Property Rules Versus Liability Rules Generally

In a famous 1972 essay Guido Calabresi and Douglas Melamed answered the general question of "property rules versus liability rules".[18] Their answer, which can be summarized easily, depends largely on the distribution of "transaction costs," i.e., the costs of arranging and completing a transaction to transfer an entitlement. According to Calabresi and Melamed, property rules are desirable in settings where transaction costs are low, and liability rules are desirable in settings where transaction costs are high.[19] Property rules are best in low transaction cost settings because they protect entitlement holders from expropriation and thereby encourage consensual transactions. In high transaction cost settings, bargaining is infeasible, so society establishes a convention under which the entitlement can be transferred at an objectively determined price. The standard liability rule, implemented by a court, provides this convention.

There is another context in which property rules are desirable because they prohibit unconditionally. That is when the activity of the injuring party is socially undesirable, no matter the scale at which it is carried out.[20] This category was implicit in the analysis of Calabresi and Melamed,[21] and has been explored more explicitly in later

[18] Guido Calabresi and Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 Harv. L. Rev. 1089 (1972).
[19] Id. 1105-1109.
[20] Keith N. Hylton, Property and Liability Rules, Once Again, forthcoming Review of Law and Economics, 2006, available at http://ssrn.com/abstract=818944.
[21] Calabresi and Melamed, supra note 15, at 1124-1127 (discussing criminal law).

articles.[22] Reckless conduct, such as joy-riding at an excessive speed through an area crowded with pedestrians, serves as an example of this property rule context.

The general scheme of tort law fits the Calabresi-Melamed theory well. Property rules, exemplified by trespass doctrine, are observed in the context of invasions to real or personal property, typically in settings in which the invader easily could have bargained with the property holder to gain access. They are also observed in cases of reckless conduct, which the law enjoins rather than simply asking for compensation.

Liability rules, on the other hand, are observed in settings such as traffic accidents, where the parties could not have bargained beforehand to arrange a price that would be paid for any specific injuries. The traffic accident setting is one of the clearest cases in which transaction costs are high. The parties to a potential traffic accident are often strangers and cannot identify each other in advance.

In recent years, the simple two-part scheme of Calabresi and Melamed has come under attack. Kaplow and Shavell,[23] providing the most forceful critique, argue that in the case of low transaction costs – fully informed agents who can identify each other and bargain over the transfer of an entitlement – it does not matter whether the property rule or the liability rule applies.[24] Under either rule, bargains will take place, and as implied by the Coase theorem,[25] economically efficient trades will occur. Kaplow and Shavell also examine a case in which the cost of meeting is low but the cost of reaching

[22] Richard A. Posner, The Economics of Criminal Law, 85 Columbia L. Rev. 1193 (1985); Keith N. Hylton (2005) The Theory of Penalties and the Economics of Criminal Law, Review of Law & Economics: Vol. 1: No. 2, Article 1, http://www.bepress.com/rle/vol1/iss2/art1.
[23] Louis Kaplow and Steven Shavell, Property Rules Versus Liability Rules: An Economic Analysis, 109 Harv. L. Rev. 713 (1996).
[24] Id. at 735.
[25] For the original presentation of the Coase theorem, see R. H. Coase, The Problem of Social Cost, 3 J. Law & Econ.1 (1960). According to the theorem, if transaction costs are low, parties will bargain their way to the efficient allocation irrespective of the initial assignment of legal rights.

agreement is high because of informational asymmetries. In this setting, they show that liability rules may dominate property rules.[26]

The critique provided by Kaplow and Shavell and others[27] has advanced the analysis of property and liability rules by incorporating a rigorous analysis of bargaining incentives. However, the results of this new literature can be reconciled with the original Calabresi-Melamed analysis. Property rules still remain preferable to liability rules in low transaction cost settings because they deter takings, even efficient ones, and thereby protect subjective components of valuation.[28] In the absence of such protection, potential victims of takings would suffer weakened incentives to invest and victims would sue or retaliate to recover losses, generating costs that would be avoided under the property rule regime.[29] However, the information asymmetry case represents a difficult set of examples that do not fit easily within the high-versus-low transaction cost framework of Calabresi and Melamed. A new synthesis should treat the information asymmetry case as an altogether new category.[30]

I think it is sufficient, in light of the new bargaining theory literature exemplified by Kaplow and Shavell, to distinguish three transaction-cost categories: *high*, *low*, and *intermediate*.[31] In addition, the costs of transacting can be split into the costs of meeting and the costs of reaching an agreement.[32] If the costs of meeting are prohibitive then transactions will not occur, and it is clearly a case of high transaction costs. If the costs

[26] Id. at 779-87.
[27] Ian Ayres and Eric Talley, Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade, 104 Yale L. J. 1027 (1995).
[28] Hylton, Property Rules and Liability Rules, Once Again, supra note 17. Even in a rigorous analysis of bargaining incentives, it still remains the case that liability rules result in expropriation, and expropriation generates social costs.
[29] Id.
[30] Id. at 5.
[31] Id. at 5-6.
[32] Id.

of meeting are low and the costs of reaching agreement high, then we have intermediate transaction costs.[33] If both the costs of meeting and the costs of reaching agreement are low, then it is a case of low transaction costs.

If, then, we distinguish cases of high, low, and intermediate transaction costs, we can state a proposition that incorporates the lessons from the bargaining theory literature along with those of Calabresi and Melamed.[34] In low transaction costs settings (where both the costs of meeting and reaching agreement are low), property rules are preferable to liability rules. In high transaction cost settings, liability rules are preferable to property rules. In intermediate transaction cost settings, either rule could dominate depending on the balance between the costs of expropriation and the costs of failed bargains.[35]

To show the greater fit or predictive capacity of this framework, consider a few of the cases that fall within the intermediate transaction cost category. One is nuisance law. The costs of meeting are low in the nuisance setting because the parties are often adjacent landowners. The costs of reaching agreement are often substantial because the precise entitlement (clean air) is difficult to define.[36] Another example is eminent domain. The cost to the government of meeting a property owner to discuss a possible purchase is low, but the cost of reaching agreement may be high because of the hold-out problem.[37] A liability rule is substituted for a property rule in both settings because the costs of

[33] The costs of reaching agreement could be substantial because of informational asymmetries or because it is difficult to define the entitlement to be transferred.
[34] Id. at 6.
[35] A liability rule allows expropriation to occur (sometimes as the result of failed bargains), which will generate social costs, either as a result of the distorted incentives of victims or from the costly litigation that follows instances of expropriation. A property rule results in a loss in allocative efficiency when a bargain fails and a wealth-enhancing transaction does not take place as a result. If the social costs of failed bargains under the property rule are less than the social costs of expropriation under the liability rule, the property rule is preferable – and conversely. See Hylton, supra note 17, at 40-42.
[36] Thomas W. Merrill, Trespass, Nuisance, and the Costs of Determining Property Rights, 14 J. Legal Stud. 13 (1995).
[37] Calabresi and Melamed, supra note 15, at 1106-1107.

property rule protection are perceived to be higher than the costs of liability rule protection.[38]

B. Choice Among Liability Rules: Strict Liability Versus Negligence

Assuming the conditions suggest that a liability rule is preferable to a property rule, the second question is: what type of liability rule? The two general types are strict liability and negligence. In mathematical models, strict liability is often treated as if it were the same as absolute liability.[39] In the same models, the negligence rule is often treated as if it were determined by comparing the benefits of additional precaution (in terms of avoidable losses) with the burden of that precaution – an approach sometimes called the "Hand formula".[40] However, in reality both the strict liability and negligence rules actually used by courts are more complicated than those captured by the mathematical models. The strict liability rules applied by courts provide justifications or defenses that an injurer can assert, rendering them far more lenient than an absolute liability rule.[41] Negligence rules also provide special justifications and defenses that allow an injurer to escape liability even when the burden or additional precaution was less than the benefit in terms of avoidable losses.[42]

---

[38] Hylton, supra note 17, at 40-42.
[39] Steven Shavell, Strict Liability versus Negligence, 9 Journal of Legal Studies 1 (1980).
[40] See, e.g., Keith N. Hylton, The Influence of Litigation Costs on Deterrence Under Strict Liability and Under Negligence, 10 Intn'l Rev. Law and Econ. 161, 166 (1990) (presenting mathematical model of negligence rule, and "Hand formula").
[41] Consider, for example, strict liability for dangerous activities, such as blasting. The Restatement (Second) of Torts provides several provisions that introduce potential defenses. See Restatement (Second) of Torts §§ 519, 520 (1977).
[42] The most obvious example of such a defense is contributory negligence. See, e.g. Richard A. Epstein, Cases and Materials on Torts 287-290 (8th ed. 2004) (explaining contributory negligence rule).

For the moment, let us adhere to the simple division between strict liability and negligence, without making any attempt to incorporate the special justifications and defenses that make legal doctrine complicated. When should we prefer strict liability to negligence?

One answer provided in the literature, from Guido Calabresi to Richard Posner to Steven Shavell, is that negligence controls only *care* levels while strict liability controls both *care* and *activity* levels.[43] By care level, I refer to the instantaneous level of care that an individual adopts when engaging in an activity. For example, one can increase his care level while driving by slowing down and watching the road ahead more closely. By activity level, I refer to the extent to which an individual engages in an activity. One can increase one's activity level in driving by using the car more frequently – say, driving three times a day rather than twice.

Under the simplest economic models, strict liability and negligence have the same effects on care levels.[44] Under either rule, an actor would always take additional care as long as the cost of that care is less than the losses avoided by that care. The reason is as follows. If additional care cost $1 and would avoid $2 in losses, the actor would clearly take that additional care under a strict liability rule. He would certainly rather bear an additional $1 in precaution costs rather than $2 in liability costs. The actor has the same incentive under negligence. The reason is that as long as the additional precaution cost is less than the losses that would be avoided, the actor would be held liable under the negligence rule. Given this, his incentives for precaution are the same under negligence as under strict liability.

[43] Guido Calabresi, The Costs of Accidents: A Legal and Economic Analysis (Yale Univ. Press, 1970); Posner, A Theory of Negligence, 1 J. Legal Stud. 29 (1972); Shavell, supra note 36.
[44] See, e.g., Shavell, supra note 36.

Now consider the level of activity. Under strict liability, the actor pays for injuries even though he has exercised the optimal level of precaution – optimal in the sense that the burden of additional precaution would be greater than the losses that would be avoided. Under negligence, the actor does not have to pay for injuries when he has exercised the optimal level of precaution. Since the overall activity costs are higher under strict liability, the actor is less likely to engage in the activity. Hence it is said that strict liability reduces activity levels while negligence does not.[45]

The activity versus care level distinction provides an explanation of the *effects* of strict liability and negligence, but it falls short of providing a positive theory of when one will encounter one rule rather than the other. For the most part, strict liability rules are limited to specific pockets of tort law. The activity-versus-care level distinction does not help us predict which pockets will be dominated by strict liability rules. One could say that strict liability should be the rule whenever it is important to control activity levels,[46] but this merely restates the question, forcing us to ask when it is important to control activity rather than care levels. And since the activity level concern is a general one, the activity-versus-care level distinction suggests that strict liability should be the default liability rule.[47]

Strict liability rules are limited to special pockets of tort law. For example, blasting in developed areas falls under the strict liability rule.[48] If you engage in blasting in a residential area you will be held liable for all losses caused by concussion and debris,

[45] See id.
[46] Indiana Harbor Belt R.R. Co. v. American Cyanamid Co., 916 F.2d 1174, 1182 (7th Cir. 1990).
[47] E.g., Keith N. Hylton, The Theory of Tort Doctrine and the Restatement of Torts, 54 Vanderbilt L. Rev. 1413 (2001).
[48] See, e.g., Spano v. Perini Corp., 250 N.E. 2d 31 (N.Y. 1969); Whitman Hotel Corp. v. Elliot & Watrous Engineering Co., 79 A. 2d 591 (R.I. 1951); Alonso v. Hills, 214 P.2d 50 (Cal. App. 1 Dist. 1950).

no matter how careful you are in conducting the blasting operation. You will not be liable to a victim who is considered "extra-sensitive" to the blasting operation, in the sense that the victim claims to have suffered a harm in an instance in which the ordinary person would have suffered no harm.[49] However, if the blasting is carried on at a level that would have caused some harm to the ordinary resident, you will be held liable for those harms caused to residents, even if they are much greater than you would have anticipated.

The blasting example illustrates a general principle: *strict liability rules are observed when the costs externalized by an activity, even when conducted with reasonable care, substantially exceed the benefits externalized by that activity*.[50] In other words, where the ratio of externalized costs to externalized benefits is unusually high, the law adopts a strict liability rule. The reason the law imposes strict liability in these cases is to deter, discourage, or shrink the activity. That explains why strict liability applies to blasting. It is an activity that imposes a significant risk of harm on individuals who live or work near the blasting operation, even when it is conducted with great care, without in most cases providing some contemporaneous benefit that makes it worth their while to tolerate those harms. By imposing strict liability, the law internalizes the harms associated with blasting and thereby discourages the use of blasting relative to other methods of destruction (e.g., wrecking ball) in areas in which harms to third parties are likely to occur.

The principle requiring comparison of externalized risks and benefits also explains why the keeping of dangerous animals, like lions, falls under the strict liability

[49] See Restatement (Second) of Torts § 524A (1977) (exempting defendant from strict liability for "Plaintiff's Abnormally Sensitive Activity").
[50] Keith N. Hylton, A Missing Markets Theory of Tort Law, 90 Nw. U. L. Rev. 977 (1996).

rule.[51] An individual who keeps a lion penned in his backyard imposes a great risk on his neighbors, while at the same time providing no significant benefit – unless, the lion holder is operating a zoo.[52] In the absence of strict liability, the benefits of holding a lion are typically enjoyed by the holder alone while the substantial costs are externalized to others (even when the holder is taking reasonable care). Strict liability corrects the lion holder's incentives by forcing him to compare his private benefits to the full costs to his neighbors.

The doctrine of *Rylands v. Fletcher* offers another illustration of the ratio test proposed here.[53] *Rylands* imposes strict liability for "non-natural" uses of land that escape and cause damage to others. In *Rylands*, strict liability was imposed on the defendant when water escaped from a reservoir constructed on his land and flooded mines on the plaintiff's land. The court argued that the storage of water under the conditions in the case imposed an extraordinary risk on adjacent landowners, greater than any reciprocal risk imposed by the adjacent land owners.[54]

The best illustration of the function of externalized benefits in the *Rylands* doctrine is given by the case of *Rickards v. Lothian*.[55] The defendant leased a commercial building with a lavatory on the fourth floor. The plaintiff was a tenant whose business occupied part of the second floor. An unknown person snuck into the building late one night, stuffed the sink, turned the faucet on full blast, and left it running overnight. The next morning, the plaintiff found his stock-in-trade (largely schoolbooks)

[51] See, e.g., Baker v. Snell, [1908] 2 K.B. 825.
[52] See, e.g., Guzzi v. New York Zoological Society, 182 N.Y.S. 257 (N.Y. App. Div. 1920), *aff'd*, 233 N.Y. 511 (1922) (distinguishing holding of bear in zoo from nuisance per se cases because of educational function); City and County of Denver v. Kennedy, 476 P.2d 762 (Colo. App. 1970).
[53] Rylands v. Fletcher, L.R 3 H.L. 330 (1868).
[54] Id. at 332.
[55] [1913] AC 263.

ruined, and brought a strict liability suit against the defendant on the theory that the introduction of the lavatory was equivalent to the reservoir in *Rylands*. The court rejected the plaintiff's claim. The court noted that "the provision of a proper supply of water to the various parts of a house is not only reasonable, but has become, in accordance with modern sanitary views, an almost necessary feature of town life."[56]

The difference between *Rickards* and *Rylands* is that the ratio of externalized benefits to externalized costs is quite different in the two cases. In *Rickards*, the provision of water supply to a building provides benefits to all who use the building. These benefits are difficult to capture in the rental fee demanded of a tenant, and it is quite unlikely that the tenant's use of water was metered with a charge that reflected the marginal benefit to the tenant of water use. Since the externalized benefits in this scenario were substantial, there is no reason to believe that the risk externalized by the introduction of a lavatory was greater than the externalized benefits. However, in *Rylands* the court had no trouble concluding that the externalized risks exceeded the externalized benefits.

It remains to fold into this analysis the function of transaction costs. *Rylands* establishes the law for a set of cases sometimes referred to as "abnormally dangerous activities",[57] and for simplicity I will refer to as "the *Rylands* cases". If transaction costs are low in the *Rylands* cases, one might argue that they should be treated as just another set of cases in which property rule protection, such as trespass law, should be adopted. However, transaction costs are higher in the *Rylands* cases than in ordinary trespass cases for several reasons. First, the injurer in the *Rylands* setting is not directly attempting to

[56] Id. at 273.
[57] Restatement of Torts (Second) § 520 (1977).

invade the victim's land. He is merely bringing something onto his own land that might escape. Second, the direction of the potential escape may not be clear, making it difficult to bargain ex ante over a waiver for the harm that might occur. A large number of potential victims creates the risk that one or more will step forward and demand to be paid off even though the risk to them is slight. Transaction costs are therefore considerably higher in the *Rylands* than in the trespass setting because of the difficulty of identifying ex ante the parties that will be injured and the nature of their injuries. For this reason, *Rylands* cases should be treated either as intermediate or high transaction cost cases.

Nuisance cases are quite similar to *Rylands* cases and should therefore be treated as equivalent in terms of the factors considered here. Transaction costs in most nuisance cases are either intermediate or high. As Merrill notes, the entitlement at stake in nuisance cases is often difficult to define (e.g., the right to clean air or absence of noise).[58] The difficulty of defining the entitlement makes it hard for parties to bargain over its value. Moreover, nuisances may generate large numbers of victims, which also makes bargaining over rights difficult.[59]

The foregoing argument can be summarized in a simple diagram. There are three transaction costs categories: high, intermediate, and low. The ratio test requires a comparison of the externalized costs to the externalized benefits (*EC* versus *EB* in the

[58] Thomas W. Merrill, Trespass, Nuisance, and the Costs of Determining Property Rights, 14 J. Legal Stud. 13 (1995).

[59] I refer specifically to the hold-out problems that would arise in this scenario. For example, if a polluter had to gain the consent of 1,000 town residents before starting production, some of the residents might realize that they could gain an advantage by holding out for a payment that comes close to the profit stream of the polluting firm. For discussion, see A. Mitchell Polinsky, An Introduction to Law and Economics 13-16 (New York: Aspen Publishers, 3d ed. 2003) (examining Coase theorem in a large numbers setting).

diagram below) connected to the injurer's activity. This framework generates six cases to consider, as shown in the box in Figure 1.

	High Transaction Costs	*Intermediate Transaction Costs*	*Low Transaction Costs*
EC>EB	Liability rule: Strict liability Property rule if injurer's activity is socially undesirable	Hybrid Property Liability rule: Nuisance (unreasonable interference)	Property rule protecting victim: trespass
EC<EB	Liability rule: Negligence	Weak Negligence: Custom defense (e.g., malpractice) Nuisance (reasonable interference	Weak Negligence: Intent to Harm (e.g., defamation) Implied Consent (e.g., assumption of risk)

Figure 1.Transaction Costs, Externalization, and Liability Rules

The "weak negligence" rules described in Figure 1 refer to areas in which there is a quasi-property rule protecting the injurer rather than the victim. For example, in the last cell (low transaction costs, externalized benefits greater than externalized costs), we encounter legal rules that require proof of intent to harm in order to find the injurer liable. Defamation is an example of such a rule. The law provides several defenses that effectively immunize tort defendants, and this was so before *New York Times v. Sullivan*.[60] Defamation law has included so many defenses that one could describe it as an area in which the plaintiff needs to show specific intent to harm in order to recover.[61] As a general rule, "information torts" such as defamation and intentional infliction of

[60] 367 U.S. 254 (1964).
[61] Oliver Wendell Holmes, Jr., The Common Law 132-42 (1881) (discussing actions for deceit and slander).

emotional distress generally fall in the category in which transaction costs are low and the externalized benefits of the defendant's activity exceed externalized costs.[62] And with respect to information torts, one typically observes substantial defenses and high burdens in the way of tort plaintiffs.

In the penultimate cell (intermediate transaction costs, externalized benefits greater than externalized costs), the negligence rule applies, but there are substantial defenses that come very close to providing immunity to the defendant. For example, medical malpractice is an area in which transaction costs can be described as intermediate, because the costs of meeting are low while the costs of reaching agreement are high because of informational asymmetry. Also, the externalized costs connected to the activity are generally less than the externalized benefits.[63] Here the law tends to favor the injurer. Although juries may sometimes be vulnerable to persuasion by plaintiff's lawyers, the law provides a substantial custom defense for doctors.[64]

The existence of defenses that virtually immunize defendants reflects a type of property rule lurking behind the categories shown in the bottom row of Figure 1. When externalized benefits are generally greater than externalized costs, the underlying

---

[62] To elaborate, because the external benefits of speech are substantial, the law has provided a subsidy, in effect, to speakers by allowing them to be held liable under an intent-to-harm rather than a negligence rule. Consider, for example, how defamation law fits within this framework. The activity level decision in the news business is the decision to publish or to publish a certain frequency. Taking care in the news business is a matter of researching claims in articles and opinion pieces with care. A strict or absolute liability standard would hold newspapers liable for any defamatory claims, whether carefully researched or not. A negligence standard would hold a publisher liable for any failure to take care in research that results in defamatory claims. An intent-to-harm standard, which is close to the real law, would hold a publisher liable only when the evidence suggests some malice or bad intent. The law adopts the most lenient standard for potential defendants, which is the intent-to-harm approach, and in doing so provides a partial subsidy to news publishers. The negligence standard would be too strict, under this paper's framework, because it fails to credit the defendant for the benefits externalized by free expression.

[63] One could represent the external cost and external benefit comparison in terms of marginal benefit and marginal cost curves. For this approach, see Hylton, A Missing Markets Theory, supra note 47.

[64] On the custom defense in medical malpractice, see, e.g, Epstein, Cases and Materials, supra note 39, at 204.

property rule should be awarded to the injurer. That is, the injurer should have a right to engage in his activity without fear of being enjoined or of strict liability. If society is made better off, after all, by the very activity that causes injury, that activity should be encouraged. As transaction costs fall, potential victims are in a better position to demand payments and to effectively enjoin the defendant's activity if the underlying property rule protects the victim, and for this reason it would be undesirable to award the property rule to the victim. The law, in effect, reverses the property rule from its usual position protecting the victim and makes it a shield for the potential injurer, by providing defenses of broad scope.

When transaction costs are high, liability rules predominate except in one instance shown in Figure 1. When the injurer's activity is socially undesirable, which means that the social costs from the injurer's activity exceed the social benefits at every scale of the activity,[65] the property rule reappears. This exception covers the case of reckless activity, or activity that presents a danger to the public such as terrorism.

IV. Application to Cyberspace

The central premise of this paper is that tort law can be applied to cyberspace wrongs in a way that is reconcilable with established tort doctrine. However, in order to do that we need to first have a clear view of the theoretical foundations of tort doctrine. The foregoing discussion sets out that view. The remaining parts apply it to cyberspace torts.

[65] In terms of marginal benefit and marginal cost curves, this would be a case in which the marginal benefit curve is below the marginal cost curve at all levels of the activity.

A. Nonconsensual Cyber-Invasions: Property Rules Versus Liability Rules

I have already described *Hamidi*, which involved the sending of thousands of messages to the employer-provided email of Intel employees, as a case involving the choice between property rules and liability rules in cyberspace. *Hamidi* is one example within a class of torts that can be called cyber-invasions. Cyber-invasions can occur in two forms. In one set of instances, the invader breaches norms governing publicly accessible information portals, such as sending spam email or collecting information from a website for a purpose that breaches the terms of a "click-through" agreement or that the information provider would find objectionable (e.g., competing against the information provider).[66] In another set of instances, the invader goes around barriers to gain access to information that is not publicly available or to alter privately-held records. I will consider these two types of cyber-invasion separately.

1. Invading a Public Information Resource

The first type of cyber-invasion I want to consider, invasion of a public information resource, involves cases such as the sending of spam email in *Hamidi*. I refer to this as a public resource invasion because the recipient of spam email holds his email box open to the public; there is no expectation or requirement that an email sender

[66] See, e.g., Intel Corp. v. Hamidi, 1 Cal. Rptr. 32 (Cal. 2003); eBay v. Bidder's Edge, Inc. 100 F.Supp. 2d 1058 (N.D. Cal. 2000); Register.com v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).

first get permission to send an email. Spam email can be viewed as an invasion because it is undesirable to the typical recipient.

Recall that in *Hamidi*, the court accepted the plaintiff's theory that trespass to chattels (i.e., trespass to personal property) was a claim that could result in a remedy of an injunction or damages against the sender of spam email.[67] However, the court held that in order to enjoin the defendant's conduct, the plaintiff had to bring evidence of substantial harm to his property.[68] Intel had produced no evidence that Hamidi's actions actually harmed the company's electronic mail system, and for that reason the court refused to enjoin Hamidi.[69]

There are other cases in which the trespass-to-chattels theory has been accepted, leading to an injunction. For example in *eBay v. Bidder's Edge*[70] the court held that the plaintiff, eBay, could enjoin Bidder's Edge from sending electronic spiders to its web site because those spiders were thought to be capable of impairing the functioning of eBay's website.

The first question raised by *Hamidi* is a general one concerning the power to enjoin. The plaintiff's power to enjoin the defendant's conduct has been a relatively murky issue in the law of trespass to chattels. The Restatement has taken the position that the plaintiff in a trespass to chattels action cannot enjoin the defendant's conduct unless he can show that it actually causes an injury.[71] However, some courts have suggested that the mere trespass to personal property gives rise to a right to seek damages

[67] Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003).
[68] Id. at 303.
[69] Id. at 303-4.
[70] 100 F. Supp. 2d 1058 (N.D. Cal. 2000).
[71] Restatement of Torts (Second), § 218 comment e, illus.2 (1977). A child climbs upon the back of B's large dog and pulls its ears. No harm is done to the dog, or to any other legally protected interest of B. A is not liable to B.

and to enjoin the defendant's conduct.[72] These courts have proceeded under the view that the law governing trespass to real property and that governing trespass to chattels should be the same.

The point at which established law gives an uncertain or doubtful answer is where theory should play a role in figuring out what the law should say. Why has the law given plaintiffs a power to enjoin under traditional (real property) trespass law? The reason, according to the theory of property rules, is to protect the plaintiff's subjective valuation of his property. If the plaintiff cannot enjoin another party's use, then that party can expropriate or destroy all or part of the value of the plaintiff's property. In view of this, there is no clear reason why the power to enjoin should be weaker in the case of personal property than it is in the case of real property.

Suppose, for example, a third party happens to find a key that matches my car's ignition. Assume I make little use of my car – say, only on Sundays – and otherwise don't see the car because it is parked in a garage far from my house. The third party uses the car without my consent and without causing any measurable or perceptible damage of any sort – e.g., he uses the car to meet his paramour for trysts. Should I lose the power to enjoin or to seek damages simply because I cannot prove that the third party's use actually damages my car? The theory of property rules suggests that I should not lose the power to enjoin, because the power to enjoin permits me to demand to be compensated for whatever subjective loss I suffer in having my car used by the third party.

[72] Blondell v. Consolidated Gas Co., 43 A. 817 (Md. 1899). Moreover, English common law did not require a showing of substantial harm in a trespass-to-chattels action. See Shyamkrishna Balganesh, Property Along the Tort Spectrum: Trespass to Chattels and the Anglo-American Doctrinal Divergence, forthcoming 35 Common L. World Rev. (June 2006).

This implies that the power to enjoin should, as a default rule, always be assumed to belong to the property holder under trespass law, whether the property is real or personal.[73] To weaken that power, as courts have done in *Hamidi* and *eBay*, is to undermine one of the fundamental protections provided by trespass doctrine. These cases declare that a liability rule remedy should replace a property rule remedy in a special setting in which property rule protection appears to be appropriate in the court's eyes.[74] The danger is that this approach could leech back into ordinary trespass rules governing real property.

The second question raised by *Hamidi* is whether property rule protection is appropriate in the circumstances. This depends on several factors, summarized earlier in Figure 1. First, *transaction costs*: the case for property rule protection becomes stronger as transaction costs fall. Second, *the direction of property rule protection has to be determined*. Property rule protection can protect either the victim or the invader. This requires a comparison of the externalized costs and benefits of the injurer's activity.

As it becomes easier for a cyberspace user to gain permission before sending an email or accessing a website (that is, as transaction costs fall), the case for protecting *someone* with a property rule becomes stronger. A property rule protecting the potential victim would be equivalent to the familiar trespass law. A property rule protecting the invader (e.g., the email sender) would be equivalent to one of the weak negligence rules described earlier. For example, it might say in effect that the person initiating the email

[73] See Richard A. Epstein, Intel v. Hamidi, The Role of Self-Help in Cyberspace?, 1 J. Law, Economics, & Policy 147, 151 (2005); Shyamkrishna Balganesh, supra note 58 (noting that English law did not require a showing of harm).

[74] To be clear, this is not to say that property rule protection really would be appropriate in the *Hamidi* or *eBay* fact settings. I am saying that the courts in *eBay* and *Hamidi* have made the confusing statement that (a) property rule protection is appropriate and (b) that in order to protect the interests at stake the only remedy they would permit is a liability rule. For an alternative description of the confusion, in doctrinal terms, see Mossoff, supra note 4, at 645.

has the right, ordinarily, to do so unless he has waived that right, or unless he knows in advance of some specific and substantial harm that the email will bring to the recipient.

As the court itself noted in *Hamidi*, this is a bit like asking whether there should be a property rule governing phone calls.[75] The answer seems relatively clear in that case. A person acquires a phone in order to communicate with others. Indeed, its value rises directly in proportion to the number of others who also have phones. A phone, a fax machine, and electronic mail system are all examples of communication portals that allow us to connect to others. Although it might be relatively cheap to contact one person in order to seek permission to place a phone call to him, in the aggregate this would be a costly system, and would destroy a substantial part of the network value of the phone system. The expense would be unnecessary, in addition, since most people would agree to being contacted by phone. If there is any property rule that is desirable in the case of telephone calls, it would appear to be one that protects the invader, i.e., the person initiating the call.

The same argument applies to the electronic mail system in *Hamidi*. Although it would be simple for one individual to contact another or a corporation to seek permission to send an email, it would be a substantial cost when viewed in light of the interest in rapid un-intrusive contact that motivates people to use electronic mail in the first place. Given the network effects that make ownership of an email account valuable, the system-wide costs of a property rule protecting potential recipients of unwanted mail could be enormous. In addition, because the whole purpose of the system is to allow rapid and widespread communication, the vast majority of users would waive property rule protection if it were given to them. Since people acquire email accounts as a

[75] Intel Corp. v. Hamidi, 71 P.3d 296, 299-300 (Cal. 2003).

communication portal, the value they perceive expropriated by the occasional unwanted email is trivial.

The upshot is that trespass, which operates as a property rule protecting the victim, is an inappropriate rule to apply to cases like *Hamidi* involving unwanted emails and to cases like *eBay* involving website access. Indeed, the reason courts have applied a diluted trespass rule (requiring substantial harm) to certain types of cyber-invasion is from a recognition of the costs of property rule protection favoring email recipients or website operators. While accepting plaintiff's trespass to chattels theory, the *Hamidi* court spoke at length about the inconveniences created by rules requiring consent in these settings.[76]

Given that a property rule protecting the victim is inappropriate, what is the proper tort rule to apply to unwanted emails? In the case of a single email or the typical email exchange, the underlying activity is one in which the externalized benefits generally exceed the externalized costs. This is true in general for "information torts" – because information is a public good, the law tends to set standards that are difficult for plaintiffs to satisfy. Since the transaction costs are, at least in a significant set of instances, low in the case of a single email, a property rule is certainly feasible in this area. The foregoing analysis suggests that the preferable property rule (assuming some type of property rule is appropriate) is one protecting the invader/email initiator. This suggests that the ideal rule in the case of an unwanted email that causes harm to the recipient would hold the email sender liable only if the evidence shows that he knew with substantial certainty that the email recipient would be harmed by opening the email.

[76] Id. at 318. However, technology could drive transaction costs so low that a system of prior consent for emails could become operational with no obstruction to the value of the network. At present, that does not appear to be the case.

Of course, with emails, as with all things, there can be too much of a good thing. Suppose, instead of a single email, we are considering a spammer who sends 50,000 emails at a time to a single server. What tort rule should apply? The spammer's activity is generally desirable in the case of a single email or reasonable number of emails. But spammers create burdens on recipients by sending thousands of emails at a time.[77] The conduct has characteristics most common with nuisances.[78] The spammer's conduct imposes external losses that often exceed the externalized gains. In addition, transaction costs are in some respects low, and in others quite high in the email context. A person who wants to engage in mass distribution of email after first gaining the consent of recipients would run into the large numbers problems that arise in nuisance settings.[79] Given these characteristics, mass email distribution that results in harm to recipients belongs in the same category as nuisances resulting in unreasonable interferences.

This analysis applies as well to *eBay*. In general, if a programmer sends electronic spiders through the internet to gather information and relay them to another source, say another website, that activity merely enhances the dissemination of information. Enhanced information dissemination allows markets to work more efficiently in allocating resources. For this reason, the externalized benefits of the programmer's conduct probably exceed the externalized costs. In addition, because of the large numbers problems encountered in the nuisance and *Rylands* settings, the transaction costs under a property rule could be quite high.

---

[77] See Mossoff, supra note 4, at 650-52 (detailing burdens imposed by spammers).
[78] The argument that the harms suffered in spam cases seem closest to the harms observed in nuisance cases, see Mossoff, supra note 4, Mark Lemley, Place and Cyberspace, 91 Cal.L. Rev. 521, 540 (2003); Edward Lee, Rules and Standards for Cyberspace, 77 Notre Dame L. Rev. 1275 (2002); Burk, O'Rourke supra note 4.
[79] I refer to the hold-out problems that would arise in this scenario, see supra note 56.

These arguments suggest that a property rule protecting the victim of spidering would be socially undesirable. For reasons similar to those given in the spammer context, nuisance theory has a better fit to the problem. If spidering occurs on a scale that disrupts the functioning of the victim's website, as the court believed had occurred in *eBay*,[80] then the injurer's activity should be deemed an unreasonable interference under nuisance theory.

An alternative theory of the harm in *eBay* is that the information dissemination itself may have been harmful to eBay because it might have steered potential users away from the eBay site.[81] This is a doubtful theory on which to award tort damages. Tort law early on took the position that competition itself does not give rise to a claim for damages.[82] If a business sets up close to a rival and charges lower prices, that rival has no claim for damages under tort law. Given this long-standing common law rule, it would seem quite strange for a court to award damages to eBay on the theory that Bidder's Edge would take business away from it by disseminating information more widely about alternatives available to potential customers.

If there is an argument for damages under this alternative theory, it would be based on the doctrine developed in business tort cases, and in ancient nuisance cases. For example, some of the earliest business tort cases, cast as nuisance cases, involved cream-

[80] 100 F. Supp. 2d, at 1071.
[81] For the most persuasive version of this argument, see Daniel Kearney, Note, Network Effects and the Emerging Doctrine of Cybertrespass, 23 Yale L. & Pol'y Rev. 313 (2005). The theory presented in Kearney's note is that in the presence of network externalities, it may be optimal to protect a monopoly. Breaking up the monopoly leads to some efficiency losses. While this theory suggests that private steps to maintain a monopoly may be socially justifiable in the presence of network externalities, it does not readily imply that the law should be altered to protect some firms (specifically those that produce a service that generates network externalities) from competition.
[82] Holmes, supra note 58, at 144-5.

skimming competition among local markets or fairs.[83] A rival who set up a fair on the road leading to an established one could be held liable for nuisance.[84] The intuition for this is that the rival's activity is a particularly discouraging form of free riding.[85] At the time when fairs were a common method of forming markets in which sellers and buyers could meet, it must have been quite costly for an entrepreneur to establish one. It would have required a great deal of effort in finding sellers and advertising to potential buyers. A competitor who waited for the entrepreneur to invest in this way, and then set up a competing fair on the most-traveled route, could easily skim away a large part of the entrepreneur's profit while investing only a fraction of the cost. If this conduct were allowed to go unimpeded, few entrepreneurs would have established fairs in the first place.

One could try to extend the reasoning of these ancient nuisance cases to the *eBay* case. However, to avoid creating a set of rules that obstruct competition, courts would have to be careful to put sharp limits on the type of case that would be viewed favorably. It would have to be a case in which the late entrant's efforts both took advantage of a substantial investment on the part of the initial entrant, and had the effect of denying the initial entrant a suitable return on his investment.[86] The misappropriation theory recognized by the Supreme Court in *International News Service v. Associated Press* provides a useful approach to setting limits to a theory based on harmful competition.[87]

---

[83] Keith N. Hylton, Antitrust Law: Economic Theory and Common Law Evolution 211 (Cambridge University Press, 2003).
[84] Id.
[85] Id.
[86] Id.
[87] See International News Service v. Associated Press 248 U.S. 215 (1918) (upholding injunction against taking news from east-coast Associated Press papers and printing it in west-coast newspapers in the competing INS network). For a discussion of the case, see Douglas G. Baird, Property, Natural Monopoly, and the Uneasy Legacy of INS v. AP, University of Chicago Working Paper, Olin Working Paper No. 246,

Property rules protecting victims of spam email or spiders are generally inappropriate, given the theoretical structure of tort law. If there is any property rule that should underlie this activity at all, it is one protecting the invader (e.g., the email sender), since his conduct is generally beneficial to society. If the victim is to be protected at all, liability rules rather than property rules should apply generally. Cases such as *Hamidi* and *eBay* seem particularly well suited for the liability rule approach exemplified by nuisance doctrine. This is not to say that property rules protecting victims could never be appropriate for cyberspace. Indeed, if transaction costs are low and the injurer's activity is of low social utility, a property rule protecting the victim could be appropriate. But the cases of invasion of a public information resource that the courts have dealt with under the trespass to chattels doctrine do not fit this description. For those cases, nuisance doctrine, not trespass, provides the better framework.

2. Invading a Private Information Resource and Always-Undesirable Activity

The second type of cyber-invasion involves going around barriers to gain access to privately-held information. For example, consider a database that is accessible only to customers who pay a fee. Suppose a non-customer gains access to the database by breaking a code that is available only to paying customers or to a certain class of

---

June 2005, available at http://ssrn.com/abstract_id=730024. The misappropriation theory seems to be applicable to cases such as EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) and Register.com v. Verio, Inc., 356 F.3d 393 (2d Cir.2004). In *Explorica*, the new competitor (Explorica) used a specially-designed search robot to gather information on prices from the incumbent firm's (EF) website, using inside information on the website's structure. Explorica used the information to undercut EF's prices. In *Register.com*, the new competitor (Verio) used a search robot to obtain information on entities that had registered their internet domain names through Register. Verio then contacted the registrants to solicit business. Some of those registrants had requested that their information not be used for solicitation purposes. Neither case was decided on the basis of the misappropriation theory.

customers.[88] Alternatively, consider the case of a psychiatrist who goes beyond the scope of her authority to peruse medical records of patients, simply to satisfy her own curiosity about them.[89] Or suppose a programmer writes a "Trojan Horse" program that invades the victim's computer by arriving as an email attachment from a familiar source, and the program then distributes information from that computer to others.[90]

Would a property rule protecting the victim, such as the trespass-to-chattels doctrine, be desirable in these cases? This question returns us to the factors that make property rules desirable. A property rule is desirable when transaction costs are low. A property rule protecting *the victim* (rather than the injurer) is desirable when the underlying activity of the injurer is externalizes more costs than benefits.

Transaction costs have to be examined in light of the reality of social intercourse. In the case of uninvited emails, the background rule governing social intercourse is one that approves of the sending of uninvited email. Individuals acquire communication portals, such as telephones or email accounts, so that they can be reached by others without first having to give those others an invitation.[91] In the cases in which the invader accesses private information, such as information protected by a code or by using a Trojan Horse to invade, there is no sense in which potential victims accept this as part of the cost of acquiring a computer that connects to the internet.[92] Any invasion of private

[88] See, e.g., Physicians Interactive v. Lathian Sys. 2003 U.S. Dist. LEXIS 22868 (E.D. Va. Dec. 5, 2003).
[89] See, e.g. Doe v. Dartmouth-Hitchcock Med. Ctr., No.CIV.00-100-M (D.N.H. July 19, 2001).
[90] Timothy L. O'Brien, Gone Spear-Phishin': For a New Breed of Hackers, This Time It's Personal, N.Y.Times, Sunday, December 4, 2005 (Sunday Business Section at pages 1 and 7).
[91] And at least in the case of telephones, the owner can take positive steps to avoid being contacted by strangers, such as refusing to allow the number to be listed in public sources. So if the owner makes the phone number available in public sources, it is fair to infer that he is willing to be contacted by strangers or by people who have not been invited to call.
[92] The consent issue is also present in the case of "spyware" software that monitors a computer user's activities. Most spyware finds its way onto computers after users click on a download button. See Blakley, Alan F., Garrie, Daniel and Armstrong, Matthew, "Coddling Spies: Why the Law Doesn't Adequately

information should be presumed to expropriate something of value unless it occurs with the consent of the invaded party. Moreover, since the cost of gaining consent is low, the cases of invaders who access private information should be treated as occurring in a low transaction cost setting. This implies that a property rule is desirable in the context of cyber-invasions of private information stocks.

Should the property rule protect the victim? As a general default rule covering tangible and intangible things, a rule protecting the possessor is superior to its alternative, because the possessor is likely to value the thing more than some other party; and a rule protecting invaders would lead countless non-possessors to threaten invasion simply to be paid off. Moreover, there is nothing generically socially desirable about the conduct of the invader in the cases of access to private information. The invader simply takes something of value to the victim rather than paying for it. The conduct is no more valuable to society than any other type of theft.

The theory of property rules suggests that property rule protection is valid in the case of an invasion of private information – Trojan Horses, surveillance, cyber-burglary in the form of breaking access codes. This implies that courts should recognize a right to enjoin even if the plaintiff cannot prove that he suffered a substantial harm. For example, the psychiatric patient whose medical records are examined by a doctor, not for treatment purposes but just out of curiosity, should be permitted to enjoin the conduct and seek

---

Address Computer Spyware", at page 4, Duke Law & Technology Review, Forthcoming Available at SSRN: http://ssrn.com/abstract=901998. Most users are unaware that by "clicking through" they have agreed to accept spyware on their machines. Id. The difficulty in the spyware case, which distinguishes it from the Trojan Horse, is that a person who "clicks through" may be saying, in effect, that they are indifferent about the spyware that may be downloaded as a result, as long as the spyware is not harmful to them. Because of this difficulty, courts considering the consent question in spyware cases have reached in consistent conclusions; see, e.g., Specht v. Netscape Communications Corp., 306 F.3d 17, 29-30 (2d Cir. 2002) (applying California law, holding that there was no consent); i.Lan Systems, Inc. v. Netscout Service Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002) (finding consent).

damages even in the absence of proof of some material injury.[93] The substantial harm requirement of *Hamidi* seems clearly inappropriate in this setting.

It follows that plaintiffs should be able to seek punitive damage awards against invaders of private information. In some cases, the victim's loss will not be easy to determine, and a punitive award may be the simplest way to motivate litigation and at the same time deter invaders. Punitive awards should be set so that they at least eliminate any prospect of gain on the part of the invader and internalize the loss suffered by the victim.[94]

Public enforcement through criminal penalties may also be appropriate in some instances involving invasion of private information resources. Invasions of private resources share a great deal in common with environmental crimes. There is often a low probability of detection, which in turn introduces collective action problems at the enforcement stage.[95] In addition, the penalties (damage awards) that will be imposed through private litigation are likely to be far too low to serve as an adequate deterrent.[96] Criminal statutes, such as the Computer Fraud and Abuse Act,[97] serve a potentially important deterrent function in this setting.

In the general analysis of property and liability rules, property rules are desirable in low transaction cost settings and in high transaction cost settings in which the injurer's activity is always socially undesirable. The discussion so far has focused on instances in which a property rule is desirable in the cyberspace context primarily because transaction

[93] E.g., Doe v. Dartmouth-Hitchcock Med. Ctr, supra note 83.
[94] Keith N. Hylton, Punitive Damages and the Economic Theory of Penalties, 87 Geo. L. J. 421 (1998).
[95] Keith N. Hylton, When Should We Prefer Tort Law to Environmental Regulation?, 41 Washburn L. J. 515, 518-19 (2002).
[96] Id.
[97] 18 U.S.C. § 1030 (2000).

costs are low. For example, the psychiatrist who uses the internet to peruse the private medical records of a patient without authorization has the option of seeking consent from the patient.

There are other examples in which the injuring party has no specific target and would therefore find it hard to gain consent. In these examples, transaction costs are high. Still, society may prefer to apply a property rule on the ground that the underlying activity of the injuring party has no social value whatsoever. One example would be posting virus-contaminated files on the internet. This is analogous to leaving a package with a bomb in a parking lot. In this case, the cost of transacting with the victim is high because the injurer does not know who the victim will be. But he does know that there will be a victim. Since the injurer's conduct has no value to society whatsoever, a property rule protecting the victim should apply. The injuring party's activity is a candidate for an injunction, and for punitive damages in the event that an injured party brings suit.

Punitive awards and criminal penalties have in common the requirement of evidence that the defendant intended to harm the victims or was at least indifferent to the victims' welfare.[98] The issue of intent may generate exceptional cases in which a cyber-invasion of a private resource has occurred and yet punitive sanctions are inappropriate. Consider, for example, the case of teenage computer prodigy who invades a private information resource in order to show his technical prowess to friends rather than cause harm to anyone or to gain an advantage.[99] The harm done by the prodigy may still be

[98] See, e.g., Kemezy v. Peters, 79 F.3d 33, 35 (7th Cir. 1996), Proctor v. Davis 682 N.E.2d 1203, 1216 (Ill. App. Dist. 1 1997).
[99] See, e.g., Bill Goodwin, "Teenage Hackers Shame IT Industry Again," Computer Weekly On-Line, May 21, 2004 available at http://www.zone-h.org/content/view/4183/31/ (virus technologist states that teens

substantial and deserving of punishment. But this example suggests that cyber-invasions of private information resources may occur in settings in which the intent to harm is lacking, which should moderate demands for punitive damages or criminal penalties.

B. Type of Liability Rule

I have argued to this point that property rules are appropriate for cyber-invasions of private information resources (e.g., Trojan Horses that steal or destroy information) and for the always socially undesirable activity of unleashing viruses. Property rules are inappropriate for cyber-invasions of public information resources (e.g., spam email).

If property rules protecting victims are generally inappropriate for cyberspace invasions of public information resources, what sorts of liability rules should be adopted, and precisely where should they be adopted? Should courts adopt strict liability, negligence, or a rule of no liability in some settings? To answer these questions, we will have to consider the different settings in which liability for cyberspace torts might be asserted.

First consider the problem of cybersecurity.[100] One could say that cybersecurity is a general problem that encompasses every case discussed in this paper. For example, perhaps better cybersecurity would have prevented *Hamidi* from distributing thousands of

---

often write and unleash viruses to show off to their friends); Chris Cobbs, "Hackers Use Their Quest for 'Trophies' to Clog Web," The Orlando Sentinel, February 11, 2000 available at http://seclists.org/lists/isn/2000/Feb/0023.html (some teenaged-boy cyberoffenders hack for bragging rights in the hacker community and to boast about their ability to wreak havoc on the web).

[100] On the economics of cybercrime and its prevention, see Mark F. Grady and Francesco Parisi, eds., The Law and Economics of Cybersecurity (Cambridge Univ. Press 2006); Neal Katyal, Criminal Law in Cyberspace, 149 U Penn. L. Rev. 1003 (2001).

emails to Intel's employees. However, I will use cybersecurity here to refer to threats posed by hackers or virus creators.

Consider just a few examples of the damage that hackers can do. The Loveletter virus, launched on May 4, 2000, altered graphic and music files, making them useless.[101] People who had spent countless hours building up electronic libraries of music found their work destroyed. The virus affected roughly 45 million computers and is estimated to have caused almost $9 billion in damage worldwide.[102] The SoBig virus is estimated to have caused almost $30 billion in losses worldwide.[103] The Klez virus caused almost $14 billion in damage.[104] In addition to viruses, the other big source of harm that has become increasingly common is theft of information. The Federal Trade Commission estimated that theft of data caused $50 billion in losses in the U.S. in 2004.[105]

It follows readily from the previous section of this paper that direct claims against hackers should be governed by property rules. A hacker is analogous, in many cases, to a vandal who spray paints someone's house. Since the hacker intends to destroy someone's property, he can seek permission before acting – in other words, transaction costs are low. In addition, since his activity is socially undesirable at any scale, it should be completely deterred rather than taxed by a liability rule.[106]

The question taken up here, which is the dominant question in the cybersecurity literature, is whether a third party should be held strictly liable for the harms caused by

---

[101] Thinkquest, Cybercrime: Piercing the Darkness (2004) http://library.thinkquest.org/04oct/00460/ILoveYou.html (accessed January 15, 2006).
[102] Id.
[103] Sharon Gaudin, September 2, 2003 Virus Damage Worst on Record for August, (http://www.internetnews.com/stats/article.php/3071051))
[104] Id.
[105] Hot Data, Economist, June 25, 2005, at 15.
[106] See, e.g., Hylton, The Theory of Penalties and the Economics of Criminal Law, Rev. Law & Econ. (2005).

hackers and virus creators – sometimes referred to as indirect liability.[107] The third parties typically mentioned are internet service providers and operating system sellers. Since they are not the authors of viruses, property rules should not be, and probably cannot be, applied against them. I will therefore consider the arguments for liability rules and for immunity below.

1. Strict Liability

As I noted before, the dominant policy issue in the cybersecurity setting is whether any third party should be held strictly liable (indirect liability) for the harms caused by hackers and virus creators. There are several third parties who could be considered candidates for liability. One is the internet service provider. Strict liability for internet service providers might lead them to monitor the activities of users, which might help them identify hackers. Another candidate is an operating system manufacturer, on the theory that it could have taken steps to reduce the damage caused by a hacker – say by fixing a security flaw in the operating system. Alternatively, in the case of a hacker who gains information from electronic files, the owner of those files could be held strictly liable.

To determine whether strict liability would be desirable, we should return to the basic principles developed in the previous part of this paper. Strict liability differs from negligence in the sense that it affects activity levels. It forces the liable party to think about how frequently it wishes to engage in the activity giving rise to liability, or to think

[107] See, e.g., Lichtman, supra note 10; Jim Harper, Against ISP Liability, 28 Regulation 1, 30, 30-33, Spring 2005.

about deep design changes that would reduce the frequency of injuries even when the activity is undertaken with optimal care.

The second basic principle is that strict liability should be applied when there is a noticeable imbalance between externalized benefits and externalized costs connected to an activity. For example, the common law applies strict liability to blasting because the ratio of externalized costs to externalized benefits is unusually high, even when the blasting is conducted with optimal care.

A key case illustrating the limits of strict liability is *Rickards v. Lothian*. Recall that an intruder gains access to the lavatory in the defendant's building and intentionally causes a flood that damages the business property of the plaintiff tenant. The court held that the defendant was not strictly liable because the activity of providing a lavatory externalized more benefits than costs to tenants of the defendant's building.

The principle illustrated by *Rickards* is evident in other cases as well. Consider, for example, the provision of natural gas. The gas is highly flammable and could cause enormous damage if it escapes. However, natural gas companies are not held strictly liable for the harmful escapes (mostly explosions in the case of natural gas) that do occur. The reason is that the provision of gas provides substantial benefits to the communities that are connected to gas supply.[108]

Now let us apply this reasoning to the virus creator. In many respects, the internet service provider is like the building owner in *Rickards*. The internet service provider allows the internet user to connect to a stream of code which includes some harmful computer viruses. Or, one could say that the operating system manufacturer is similar to

[108] Strawbridge v. The City of Philadelphia, 2 Pennyp. 419 (Pa. 1880); Foster v. City of Keyser, 501 S.E. 2d 165 (W. Va. 1997); Mahowald v. Minnesota Gas Co., 344 N.W.2d 856 (Minn. 1984).

the building owner in *Rickards*, while the internet service provider is similar to the water supply company. The unknown wrongdoer who stuffs the sink and turns on the water is closely analogous to the virus creator or hacker.

This analogy suggests the conclusion that the internet service provider and operating system manufacturer should not be held strictly liable for the conduct of the hacker. They have jointly provided an information resource that benefits the internet user, just as the water provision in *Rickards* benefited the plaintiff. Moreover, given that the potential harmful resource in the virus case is information, public goods theory suggests that strict liability would be inefficient given the external benefits associated with enhanced information dissemination.[109]

Although my focus to this point has been on viruses and hackers, the question whether strict indirect liability is socially desirable has arisen in the context of copyright violations and file sharing over the internet. The foregoing argument against strict liability applies to the claims for copyright infringement liability against the developers of peer-to-peer file sharing networks, which was considered in *MGM Studios, Inc. v. Grokster, Ltd.*[110] Since peer-to-peer file sharing networks clearly have socially desirable uses, the developers should not, as a general policy, be subject to indirect strict liability for infringement.[111]

2. Negligence

[109] Hylton, A Missing Market Theory, supra note 47, at 988; Richard A. Posner, The Economics of Justice 262 (1981). See also Holmes, supra note 58, at 139 (suggesting that legal standard for slander is biased to favor the defendant because of the benefits of free speech).
[110] 545 U. S., 125 S.Ct. 2764 (2005).
[111] The alternative enforcement strategy available to the music industry is individual lawsuits against music downloaders. For an empirical analysis of the effectiveness of that strategy, see Sudip Battacharjee, Ram D. Gopal, Kaveepan Lertwachara, and James R. Marsden, Impact of Legal Threats on Online Music Sharing Activity: An Analysis of Music Industry Legal Actions, 49 J. Law & Econ. 91-114 (March 2006).

What about the option of liability based on negligence? As a general rule, the answer to this question is yes. The negligence standard is the default liability rule in tort law. Islands of strict liability and those of tort immunity appear to be relatively infrequent exceptions encountered in a sea of negligence law. However, even on this question we have to consider the specific form of the negligence charge, including possible defenses.

Negligence assertions come in three general forms. One is negligence in *operation*, a charge that the defendant was negligent in his conduct, e.g., in operating a car. A second is negligence in *design*, a charge that the defendant was negligent in the manner in which he designed some object that played a role in causing the plaintiff's harm. The third is negligence in *informing* or *warning*, a charge that the defendant was negligent in failing to inform the plaintiff of a foreseeable injury. In the case of a claim of indirect liability for a virus, the defendant operating system seller typically has taken no positive action in the course of its routine that led directly to the harm. As a consequence, the types of negligence charges against the operating system seller usually will be either negligence in design or negligence in warning. In the case of the internet service provider, all three types of negligence claim might be available to a plaintiff.

Negligent design and warning claims include, as special cases, most product liability actions. Product liability lawsuits are often described as strict liability. However, product liability lawsuits based on defective designs and warning failures are grounded in negligence doctrine rather than strict liability. The only category of product liability claim in which truly strict liability is observed is that involving manufacturing

defects – i.e., glitches in the manufacturing process that result in 1 out of every 1000 or so products being defective.

3. Proximate Cause and Intervention

The negligence in design issue was addressed in *Rickards*. The plaintiff had received an award from the trial court on the ground that the defendant could have used an alternative sink design that would have reduced the likelihood of harm to the plaintiff. The House of Lords reversed this part of the trial court's decision, holding that intervention on the part of the unknown wrongdoer severed the chain of causation between the defendant's negligence and the plaintiff's harm.[112] In other words, the court held that the defendant's negligence in design was not a *proximate cause* of the plaintiff's harm, given the intervention of the sink stuffer.

The intervention holding in *Rickards* is consistent with the traditional view courts took at the time of that decision to the proximate cause question, when the harm was caused by intentional intervening conduct. During the nineteenth and early twentieth centuries, courts tended to treat intentional interventions such as that observed in *Rickards* as sufficient to prove lack of proximate cause – though there were exceptions to this approach even then. Modern cases have begun to take a less rigid approach.[113]

[112] [1913] A.C. 263, at 282.
[113] This progression in the cases is suggested by the proximate cause cases covered in most law casebooks. See, e.g., Epstein, Cases and Materials on Torts, chapter on proximate cause. See also, William L. Prosser, Handbook of the Law of Torts, 267 (4th ed., West Publishing Co., 1971) (predicting "ultimate victory" of general foreseeability test in proximate cause case law).

Some jurisdictions, for example, have held car owners liable when they have negligently left their keys in the car and a thief has stolen the car and injured a pedestrian.[114]

Courts have yet to articulate a clear principle distinguishing cases in which a defendant will be held liable for the intentional acts of an intervening party.[115] However, the cases do suggest some factors that make liability more likely. One is the case in which the plaintiff has relied on the defendant to take steps to prevent the very injury that occurs. For example, in *Janof v. Newsom*,[116] the plaintiff employer relied on the employment agency to do a background check on the potential employee. The agency recommended a potential employee without conducting an investigation, and the employee robbed the plaintiff.

The reliance factor suggests that the harm that occurs to the victim is highly foreseeable. When a potential victim of some harm relies on another person to take steps to prevent that harm, the potential victim often forgoes self-protective steps that they would ordinarily have taken. In *Janof*, the plaintiff employer conducted no background search on his own because he assumed the employment agency would do a search, and bring to his attention any problems or not recommend the potential employee at all. The principle suggested by *Janof* is that if the plaintiff's reliance is of a degree that the plaintiff forgoes significant self-protective steps that he would ordinarily take, because of reliance on the defendant's efforts, then the intervention of a third party will not sever the chain of causation between the defendant's negligence and the plaintiff's injury.

Another set of cases in which courts have found the defendant liable in spite of third party intervention is when the defendant's negligence effectively disables or leaves

[114] E.g., Ross v. Hartman, 139 F. 2d 14 (D.C. Cir. 1943).
[115] Prosser, Handbook of the Law of Torts, chapter 7 (1971).
[116] 53 F.2d 149 (D.C. Cir. 1931).

the plaintiff in a position where he or she cannot take steps to avoid the harm, and the defendant itself could have protected the plaintiff from the harm. For example, in *Brower v. New York Central & H.R.R.*,[117] the railway defendant negligently collided with the plaintiff's horse-drawn wagon. The wagon was destroyed, as was the horse, and its contents were strewn about the street. The plaintiff remained in a state of shock as thieves came along and ran off with his property. The railway's security agents stood guard to protect the train as all of this was occurring. Another case with the same general characteristics is *Hines v. Garrett*,[118] where the defendant railway negligently passed the plaintiff's stop and let her off almost a mile away from it, requiring her to walk through an unsettled area. The plaintiff was raped as she tried to walk back to her intended destination.

Janof, *Brower*, and *Hines* are all cases decided in the period in which courts tended to adhere to the traditional view that intervention by a third party breaks the chain of causation between the defendant's negligence and the plaintiff's injury. They establish clear exceptions to the intervention rule. More modern cases tend to rely on the general concept of foreseeability, which does not provide clear doctrinal guidelines.

Returning to the cyberspace problem, how should the intervention of a hacker be treated? Suppose a plaintiff brings suit against an internet service provider or operating system seller on the theory that the defendant should have taken greater precautions to avoid the harm caused by the hacker. Should the intervention of a hacker be treated as severing the chain of causation between any negligence on the part of the defendant and the plaintiff's injury?

---

[117] 103 A. 166 (N.J. 1918)
[118] 108 S.E. 690 (Va. 1921)

The question of intervention in the cyberspace setting can be approached in light of the traditional rules or in light of the modern foreseeability approach. The former approach is much more predictable, since the cases give fairly clear exceptions to the rule that intervention severs the causal chain. The later cases require a fact specific inquiry, the outcome of which probably could not be predicted in the absence of a real case. For this reason, I will focus on the traditional rules in this part.

The traditional rules suggest that the answer to the question of intervention depends on the type of negligence that is asserted and proved in court. *Janof* suggests that if the plaintiff reasonably relied on the defendant taking some particular precaution, and for this reason failed to take care on his own, the defendant could be held liable even though the injury resulted from the intervention of a third party. In the cyberspace context, this means that an internet user could recover from an internet service provider if the user relied on the provider for some precaution, thereby failing to take precaution himself, and suffered a loss as a result of a computer virus.

The question this takes us to is whether there are instances of such reliance in the cyberspace setting. Clearly, it is an empirical question and cannot be answered on the basis of armchair speculation. A real case would have to present a set of facts that bring this question to life. However, in most run-of-the-mill cases of virus contamination, internet users are not relying on a particular precaution taken by an internet service provider or operating system seller. If I choose to download a file from the Social Science Research Network electronic library, a warning appears telling me that it could contain a virus. After seeing the warning, I choose whether to download the file. In this scenario, I do not rely on a specific precaution taken by the internet service provider or

operating system seller. Even if no warning were provided, it is now common knowledge that a file downloaded from a website could contain a virus. Armed with common knowledge, or informed by the warning, I have no reason to rely on some special precaution taken by the internet service provider or by the operating system seller.[119]

Again, the answer to the reliance question is in the end an empirical matter. We might have a different case if I had approached an internet website to download a file and had a reasonable basis for believing that in the absence of a pop up warning my operating system would not be exposed to a computer virus. Suppose, for example, I had been trained into relying on the warning, and one did not appear when it should have (for example, when I went to download a paper from the Social Science Research Network website). These might present cases in which the design flaw exposes the operating system seller to liability, though it would be difficult for the plaintiff to show that he reasonably relied on the warning given the circumstances. Since most computer users know that a virus can be contracted by downloading a file (and software licenses waive legal claims for such harms), it would be difficult for a plaintiff to prove that it was reasonable for him to assume that it was perfectly safe to download a file from the internet.

The other basis for holding the defendant liable in spite of the third party's intervention is the case in which the defendant's conduct disables the plaintiff from taking precaution, leaving him vulnerable to the third party.[120] Suppose, for example, a design flaw in a security patch disables the operating system's defenses or renders the

[119] It is also true that the software license disclaims any responsibility for harm caused by third parties, which is another reason that some level of assumption of risk is likely to be found in this case.
[120] See, e.g., Demon in the Machine, Economist, December 3-9. 2005, at 59 ("millions of CDs sold by Sony BMG surreptitiously contained a secretive computer program to prevent copying on a PC – yet left around 500,000 computers vulnerable to viruses".)

operating system especially vulnerable to a particular virus. The user downloads the security patch and his computer contracts the virus. This might be considered analogous to cases like *Brower* and *Hines*, where the defendant's negligence puts the plaintiff in a particularly vulnerable position with respect to the intervening wrongdoer.

Now consider the general foreseeability test as a way of determining whether an internet service provider or operating system seller should be liable for the harms caused by a hacker or virus creator. Instead of looking at particular types of negligence in conjunction with reliance or the disabling of the plaintiff, we should now consider any possible fact scenario in which a court might hold that the defendant should have taken a precaution in order to prevent a harm caused by an intervening party.

As I noted before, the general foreseeability approach is fact specific and could easily lead to (or not lead to) liability depending on how courts weigh the costs and benefits of a particular precaution. Because of the uncertainty surrounding this approach, the only useful thought exercise that can be conducted at this stage is to consider the general type of negligence asserted and the likely defenses.

The most general type of negligence assertion is that the internet service provider failed to take precautions or the operating system seller failed to correct some flaw in its software that left users vulnerable to the work of a hacker. Since software design is imperfect, and since hackers search for ways to exploit security flaws, I assume there are many potential fact scenarios that could be asserted to support such a negligence claim. Moreover, in each case, it might appear from a hindsight-based test that the defendant was negligent. After all, software code is just code. Presumably any competent programmer could correct a flaw, viewed in isolation, once it has been identified. Since

the cost of correcting a particular flaw would appear to be low (just write some more code), and the possible harm to the victim potentially high, the plaintiff's negligence theory would appear to be plausible.

But this analysis of a hypothetical negligence claim is incomplete, for several reasons. First, measuring the burden of precaution by looking at the cost of fixing an isolated flaw is probably incorrect on economic grounds. Second, fixing flaws or preventing hacker attacks requires a level of intrusion that raises troubling issues on its own.[121] Third, given that the enemy is difficult to identify and constantly changing its strategy, any precaution taken must avoid making the problem worse.

The burden of precaution involved in fixing a software flaw probably looks low to most people on a hindsight-based test. But with a complicated, evolved, software product, such as an operating system, the precaution cost probably should not be measured in isolation. If there are *N* functional components in communication with each other, then a hacker presumably has something like *N!* ways to exploit a flaw in one component in order to contaminate or damage the whole system. After one particular path has been chosen, the fix seems cheap. But before a particular path has been chosen, the fix is quite difficult.

In addition to the burden being potentially enormous, the level of intrusion required to fix a flaw or prevent an attack raises troubling issues. An operating system seller can make a security patch available, but in the absence of prior consent cannot install it on its own or force a computer user to install it. An operating system seller or an

[121] See, e.g., Harper, supra note 96.

internet service provider might be able to identify a hacker.[122] But the seller or provider, short of passing information to government authorities, has no legal authority to prevent the hacker from accessing the internet – and even attempting to do so would be futile, since the hacker could always gain access from an alternative site. And if an operating system seller or internet access provider were somehow to block internet access to users meeting a certain profile, even in a case in which it leads to an unambiguous improvement in society's welfare, most people would be concerned about the loss of privacy and freedom of expression this would entail. This is a part of the burden of preventing hacker attacks.

The information market concerns that would lead one to be wary of imposing a duty on an internet service provider or operating system seller to prevent hackers from launching attacks might seem to suggest that the standards for information torts (e.g., defamation, intentional infliction of emotional distress) would be appropriate for determining indirect liability for hacker attacks. However, these standards are not directly applicable to the case of indirect liability. The liability standard for information torts such as defamation is a difficult one for plaintiffs to meet, but that is because it is the defendant's activity that brings information to the market. In the case of a hacker or virus creator, the complaint against the operating system seller or internet service provider is not related to bringing information to the market. The complaint is that it should have taken steps to prevent one individual from harming another. Information

[122] Of course, one question here is whether a private party will have an incentive to identify a hacker. Operating system sellers and internet service providers are repeat players, and therefore should have strong incentives to identify hackers. Private firms that hold records are not necessarily repeat players, and therefore may not have strong incentives to identify hackers. Resources that record-holding firms invest in identifying hackers provide benefits to other firms, including rivals. For this reason, record-holding firms may have inadequate incentives to identify hackers. For an economic analysis of this issue, see Bruce Kobayashi, An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goods, 14 S. Ct. Econ .Rev. 261 (2006).

market concerns are relevant but not a controlling factor here in determining the proper liability standard.

An analogous case involves the duty of a psychologist to take steps to protect a third party who is named by one of the psychologist's patients as the target of a planned assault. In *Tarasoff*,[123] the court imposed a duty to warn the potential victim when the patient makes a credible threat involving a specific targeted individual. *Tarasoff* remains controversial because of the concern that a duty to warn would discourage open dialogue between the patient and his therapist. In this respect, *Tarasoff* reflects the information-market concerns observed in the area of information-based torts such as defamation. However, courts following *Tarasoff* have attempted to strike a balance between the information-market concerns and the goal of minimizing harm by requiring warnings only in instances of specific and credible threats.[124]

The principle of *Tarasoff* appears to apply to the case of the hacker and the third parties who could prevent his attacks. Moreover, the principle would appear to apply whether the third party attempts to prevent the hacker from acting or to warn the potential victim. It may be feasible for an internet service provider or operating system seller to prevent some hacker attacks by monitoring internet activity. However, because of the information-market concerns (loss of privacy, control of expression), this sort of intervention is easier to defend if the internet service provider has reliable information involving credible threats against a specific target. Of course, even under these circumstances, it may be impossible to prevent a hacker from launching an attack.

[123] Tarasoff v. Regents of University of California, 551 P.2d 334 (Cal. 1976).
[124] See, e.g., Hedlund v. Superior Court, 669 P.2d 41 (Cal. 1983); Thompson v. County of Alameda, 27 Cal. 3d 741 (Cal. 1980); Davidson v. City of Westminster, 32 Cal. 3d 197 (Cal. 1982).

Warning the potential victim is an obvious precautionary option that has the benefit of appearing not to be a futile exercise. But the usefulness of a warning depends on the circumstances.[125] If it is infeasible to issue a warning in time to prevent the attack, then it cannot be considered a useful precautionary step, and no court should impose a duty to warn under these conditions. In addition, a warning may backfire by creating the very problem the operating system seller or internet service provider is trying to avoid. For example, a warning to potential victims that tells them that their operating systems have a specific vulnerability and need to be patched may spur a hacker to try to exploit the vulnerability. The usual procedure in the industry is for a security patch to be developed and made available to computer users without broadcasting the existence of a particular vulnerability.[126] However, the presumably rare case in which an internet service provider or operating system seller obtains information about a specific attack planned against a specific target would appear to be one in which a duty to warn would be appropriate, as in *Tarasoff*. Whether the failure to give a warning in such a case would be negligent is a different issue, and would depend on the burden and likely effectiveness of warning.

C. Immunity

[125] On the economics of cyber-attack warnings, see Peter P. Swire, A Model for when Disclosure Helps Security: What is Different about Computer and Network Security, in Grady and Parisi, eds., supra note 100.

[126] Ashish Arora, Rahul Telang, Hao Xu, Optimal Policy for Software Vulnerability Disclosure, at page 2,Working Paper in SSRN electronic library, 2004, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=669023.

The information market concerns lead naturally into a discussion of the immunity issue exemplified by *Blumenthal v. Drudge*. Recall that America Online was held immune to a defamation claim brought by Sidney Blumenthal because it was protected by Section 230 of the Communications Decency Act (CDA).[127] Given that America Online's relationship to Drudge was indistinguishable from that between the New York Times and one of its columnists, the outcome of *Blumenthal* is difficult to defend. It is a long-settled matter of law that publishers are vicariously liable for the statements of the writers whose work they publish.

The general issue raised by *Blumenthal* is the extent to which internet service providers should be vicariously liable for the content that they make available to their subscribers. While *Blumenthal* appears to be a case in which vicarious liability would have been found in the absence of the protecting statute, a more troubling case involves statements posted in online discussion areas (bulletin boards, or chatrooms). The CDA certainly protects internet service providers from liability in those cases as well, but I am now asking whether there is a basis in tort doctrine for this protection.

The immunity question returns us to *Rickards v. Lothian*. The anonymous person who posts a false negative comment about your business in an online bulletin board can be analogized to the unknown sink stuffer in *Rickards*. The internet service provider's general activity, including the provision of the online bulletin board, is beneficial to society – like the provision of water in *Rickards*. The principle reflected in *Rickards* suggests that internet service providers should not be vicariously liable for defamatory

[127] Communications Decency Act of 1996, 47 U.S.C. § 230 (2000).

comments posted in online discussion areas over which they assert virtually no control.[128] But this is different from the *Blumenthal* case, where the internet service provider did control the content. To make *Blumenthal* similar to *Rickards*, we would have to change the facts of *Rickards* so that the defendant building lessee actually stuffs the sink. And if the defendant stuffed the sink in *Rickards*, he would clearly be liable for the damage done to the second-floor tenant.

The Communications Decency Act was a reaction to the failure of at least one court to draw the distinctions just drawn between appropriate and inappropriate cases for vicarious liability.[129] The statute itself was an overreaction that has led to a far broader immunity shield than would be implied by common law tort doctrine.

The last real-world problem to consider is liability for theft of information. The issues here are in some instances academic since cases of information theft do not always lead immediately to a substantial and quantifiable harm to the victims.[130] If someone steals your medical records, what is the harm to you? Obviously, if someone steals your "medical identity" and uses it to obtain fraudulent prescriptions, there is a potential harm if you are required to pay for those prescriptions or if the identity thief's conduct prevents you from obtaining your medicine. But if they take your information and never reveal it to anyone, you have arguably suffered no harm.

---

[128] This principle was initially followed in Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991). For a more recent case consistent with the principle but decided on the basis of the CDA, see Carafano v. Metrosplash.com, Inc, 339 F.3d 1119 (9th Cir. 2003).

[129] Stratton Oakmont Inc. v. Prodigy Services Co., 1995 WL 805178 (N.Y. Sup. Ct. 1995). The House Conference Report on the Communications Decency Act states, "[o]ne of the specific purposes of [section 230 of the Act] is to overrule Stratton-Oakmont v. Prodigy…" H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.). See also, Jay Zitter, Liability for Internet Service Provider for Internet or E-mail Defamation, 84 A.L.R.5th 169 (2000).

[130] See Thomas M. Lenard and Paul H. Rubin, Much Ado About Notification, Regulation, 44-50 (Spring 2006) (assessing costs of identity theft).

Given the imprecise and inchoate nature of the injury to victims, there is the possibility that firms that hold information electronically may take inadequate steps to prevent its theft.[131] After all, if the information is stolen, it may take a long time before some victim becomes aware of some way that they have been harmed as a result.

In spite of the imprecise and inchoate nature of the injury, tort law should be sufficient to regulate the incentives of data holders.[132] Cases of information theft would appear to be ideal for class action attorneys. They involve small losses spread across large numbers of victims. There is nothing to prevent courts from estimating the potential losses to victims and forcing the negligent data holder to set up a fund to compensate those losses.[133] Where the information holder has been negligent, the penalty generated by class action litigants should be large enough to deter future negligence. Moreover, this is in theory superior on deterrence grounds to a scheme involving statutory penalties, because the damage judgments awarded in class actions will have a closer fit to the actual harm suffered by victims than would statutorily-set penalties.

A potentially superior approach to class actions seeking compensatory damages would be restitution-based claims against corporations that failed to protect personal information. If, for example, a corporation has profited from permitting the personal

---

[131] As Bruce Kobayashi suggests, they are likely to have inadequate incentives to identify hackers, see Kobayashi, supra note 118. In addition to this problem, if the harm to victims is difficult to predict and likely to appear many years after the data security breach occurs, firms may choose to ignore the risk of liability for data security breaches.

[132] An alternative to tort law is to permit the reputation market to pressure firms to protect personal data. In order for the reputation market to work, data breaches would have to be disclosed in a way that signals the importance of the breach. See Schwartz, Paul M. and Janger, Edward J., "Notification of Data Security Breaches" Michigan Law Review, Vol. 105 Available at SSRN: http://ssrn.com/abstract=908709.

[133] Obviously, there should be a concern for fraud under this system. The losses should be estimated by competent analysts and supported by credible evidence. The widespread fraud observed recently in the silicosis litigation should not be permitted to occur in this area. On the silicosis fraud, see Silicosis Ruling Could Revamp Legal Landscape, by Wayne Goodman, http://www.npr.org/templates/story/story.php?storyId=5244935.

information of customers to be stolen,[134] plaintiffs should be able to bring a claim for disgorgement of the corporation's gains from that theft. In addition, if the corporation's conduct can be characterized as intentional, a punitive award should be added to the restitution-based judgment. Specifically, the punitive award should be a multiple of the disgorgement remedy, with the multiple set in order to offset the prospect that the defendant might have escaped liability because of the low probability of detection.[135]

V. Conclusion

This paper has applied the theory of property rules and liability rules to cyberspace torts. That theory suggests that trespass doctrine is appropriate in instances of cyber-invasions of private information resources, such as the breaking of codes to access private information on the web. However, trespass doctrine should play no role in instances of cyber-invasions of public information resources, such as the sending of unwanted emails in *Hamidi* or the information gathering in *eBay*. Cyber-invasions of public information resources can be analogized either to nuisance or to negligence cases. Nuisance doctrine appears on both theoretical and practical grounds to provide the best fit.

Another set of cases that might lead to liability are those in which plaintiffs assert indirect liability claims against operating system sellers or internet service providers for

[134] Suppose, for example, a retailer encourages customers to apply for gift cards, and an identity thief applies for several thousand dollars worth of gift cards and spends them quickly. If the store's security system is so weak that these events occur frequently, a plaintiff's lawyer could take the high frequency of occurrence as evidence that the retailer either recklessly or intentionally permitted identity theft to occur. For a journalistic account of the various identity theft scams and recent case law, see Jason Krause, Stolen Lives, ABA Journal, March 2006, at 36.

[135] Keith N. Hylton, Punitive Damages and the Economic Theory of Penalties, 87 Geo. L. J. 421, 439-444 (1996) (setting out algorithm for punitive awards).

the harms caused by certain actors (virus writers, copyright violators). The theory presented here suggests that the basis for strict indirect liability is weak. Negligence principles apply here, as elsewhere, though special attention should be given to proximate causation issues and the peculiar burdens of preventing virus attacks. Finally, the theory suggests that immunity rules should also play a role in this area, though in a much smaller set of instances than those protected by the Communications Decency Act.