2006

14 S. Ct. Econ. Rev. 221

**LENGTH:** 17470 words

ARTICLE: **Holding Internet Service Providers Accountable**

**NAME:** Doug Lichtman and Eric Posner *

**BIO:**

* Doug Lichtman, Professor of Law, University of Chicago Law School, d-lichtman@uchicago.edu. Eric Posner, Kirkland and Ellis Professor of Law, University of Chicago Law School, eric_posner@law.uchicago.edu. This paper was prepared for "The Law and Economics of Cyber Security" conference held on June 10, 2004, at George Mason University School of Law. It ultimately formed the basis for an amicus brief filed at the Supreme Court as part of the Grokster litigation. See Brief of Kenneth J. Arrow et al, MGM Studios, Inc v Grokster, Ltd, No 04-480 (2005). For helpful comments, we thank conference participants, especially Amitai Aviram, Emily Frye, Neal Katyal, and Peter Swire, as well as readers Wayne Hsiung, Orin Kerr, Saul Levmore, Lior Strahilevitz, and Alan Sykes. Lastly, for financial support, Posner thanks the Russell Baker Scholars Fund; Lichtman thanks Merck & Co., Inc., Microsoft Corporation, Pfizer, Inc., PhRMA, Verizon, and Visa U.S.A., Inc.

**SUMMARY:**
*... Internet service providers are today largely immune from liability for their role in the creation and propagation of worms, viruses, and other forms of malicious computer code. ... Our argument in favor of service provider liability is primarily based on the notion that ISPs are in a good position to reduce the number and severity of bad acts online; and that intuition finds support even within the aforementioned immunity and safe harbor statutes. ... Part III considers in more detail the two primary objections sketched above, namely: (1) that liable ISPs will be overly cautious and thus inefficiently exclude marginal subscribers; and (2) that liability will reduce user incentives to engage in efficient self-help. ... Importantly, note that where activity level is the concern, strict liability is often appropriate, in that the logic of liability is not at all tied to any negligent failure on the part of the indirectly liable party to take some cost-justified precaution. ... Even outside of any contractual obligations, it is typically in a subscriber's own interest to protect his computer, at least to the extent that precautions are not too cumbersome. ... On this same theme, note that nothing that we say about indirect liability for ISPs is meant to suggest that Internet subscribers should themselves be immunized from liability. ...*

**HIGHLIGHT:**

*Internet service providers are today largely immune from liability for their role in the creation and propagation of worms, viruses, and other forms of malicious computer code. In this essay, we question that state of affairs. Our purpose is not to weigh in on the details--for example, whether liability should sound in negligence or strict liability, or whether liability is in this instance best implemented by statute or via gradual common law development. Rather, our aim is to challenge the recent trend in the courts and Congress away from liability and toward complete immunity for Internet service providers. In our view, such immunity is difficult to defend on policy grounds and sharply inconsistent with conventional*

*tort law principles. Internet service providers control the gateway through which Internet pests enter and reenter the public network. Service providers should therefore bear some responsibility not only for stopping malicious code, but also for helping to identify individuals who originate it.*

**TEXT:**

[*222] **I. INTRODUCTION**

Computer viruses and related strains of Internet contagion impose a significant cost on the many individuals and entities that rely on Internet access for commerce, research, and communication. The United States government has responded to this problem with efforts to identify and deter those who create and propagate Internet pests. Thus, for example, both the Federal Bureau of Investigation and the Department of Homeland Security allocate substantial resources to the battle against cyber-crime; and Congress has passed a number of criminal statutes designed to target the troublemakers who create Internet viruses and other forms of malicious computer code. [1] Government efforts along these lines have been augmented by the actions of private parties as well. Microsoft, for example, has offered cash rewards for any information leading to the arrest and conviction of those responsible for particularly disruptive Internet attacks, [2] and many computer hobbyists volunteer to help trace the sources of Internet mischief.

These tactics obviously have the potential to reduce the total amount of harm caused by cyber-insecurity; however, we doubt that direct intervention aimed at perpetrators of Internet mischief can be a sufficient response. Our concern is that the perpetrators of cyber-crime are too often beyond the effective reach of law, both because these individuals are almost impossible to track, and because, even when identified, these individuals usually lack the resources necessary to pay for the damage they cause. Thus, in this essay, we join a growing chorus of legal commentators [3] in arguing that attempts at direct intervention must be supplemented by a legal rule that brings Internet service providers (ISPs) into the chain of responsibility. Specifically, ISPs should to some degree be held accountable when their subscribers originate malicious Internet code, and ISPs should also to some degree be held accountable when their subscribers propagate malicious code by, for example, forwarding a virus over email or adopting lax security precautions that in turn allow a computer to be co-opted by a malevolent user.

[*223] This might sound harsh. But rules that hold one party liable for wrongs committed by another are the standard legal response in situations where, as here, liability will be predictably ineffective if directly applied to a class of bad actors and yet there exists a class of related parties capable of either controlling those bad actors or mitigating the damage they cause. Phrased another way, while indirect liability comes in a wide variety of flavors and forms--strict liability and negligence; explicit statutory provisions and also more flexible common law standards; and so on--it is the norm, and we do not see any reason why legal rules associated with cyber-security should be an exception to the pattern of rules that govern structurally identical interactions throughout the offline world.

Our position admittedly runs counter to recent legal trends. In section 230 of the Communications Decency Act of 1996, for example, Congress announced that a provider of "interactive computer service" is not to be treated as "the publisher or speaker of any information provided by another information content provider," [4] in many ways immunizing Internet service providers from liability for defamatory content that is provided by business partners or customers but disseminated by the service itself. Similarly, the Digital Millennium Copyright Act of 1998 sharply limits a service provider's liability for copyright infringement in cases where the service provider merely acts as a conduit for the incriminating material, [5] and that statute more broadly limits liability in instances where the service provider did not know about the infringing activity, was not aware of facts or circumstances from which the activity would be apparent, did not receive a direct financial benefit from the infringement, and acts in accordance with statutory guidelines to expeditiously disable access to the material in question. [6] Courts interpreting these provisions have reinforced this apparent trend away from ISP liability by, among other things, interpreting these statutes to preempt state laws that would otherwise have encouraged ISPs to take due

care. [7]

Then again, maybe these trends are not as one-sided as they at first appear. Our argument in favor of service provider liability is primarily based on the notion that ISPs are in a good position to reduce the number and severity of bad acts online; and that intuition finds support even within the aforementioned immunity and safe harbor statutes. [8] [*224] So, for example, while the Communications Decency Act does remove the specter of indirect liability for the transmission of indecent or defamatory content, the act also encourages Internet service providers to address inappropriate content through voluntary private action. To that end, one provision immunizes service providers from liability for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." [9] On this same theme, not only is much of the immunity available under the Digital Millennium Copyright Act contingent on a service provider's efforts to quickly remove content plausibly associated with infringement, but also, like the Communications Decency Act, the Digital Millennium Copyright Act protects service providers from "any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing." [10]

In any event, ours is not an argument about the state of the positive law nor an attempt to divine Congressional intent. Our point is simply that, faced with the growing problem of cyber-insecurity, ISPs should be called into the service of the law. Much as the threat of liability puts pressure on the owners of bars and restaurants to watch for any copyright infringement that might take place within their establishments; [11] and the common law principle of vicarious liability obligates employers to monitor, train, and otherwise exercise control over the behavior of their employees; [12] common law tort liability or more carefully tailored federal statutes should be used to encourage ISPs to do their part in responding to Internet worms, viruses, denial-of-service [*225] attacks, and the like. Service providers control the gateway through which Internet pests enter and reenter the system. As such, service providers can help to stop these pests before they spread and to identify the individuals who originate malicious code in the first place. ISPs should be required by law to engage in these precautions.

We anticipate two primary objections. The first--and a concern that is repeated throughout the literature--is that liability will cause Internet service providers to overreact. As Neal Katyal puts the point, "Because an ISP derives little utility from providing access to a risky subscriber, a legal regime that places liability on an ISP for the acts of its subscribers will quickly lead the ISP to purge risky ones from its system." [13] Assaf Hamdani similarly worries that ISPs will inefficiently exclude some users because "ISPs do not capture the full value of the conduct they are entrusted with policing." [14] These arguments are in our view misstated, as in every market where goods are sold at or near marginal cost the relevant seller "derives little utility" from the sale; and in every market where the market price is less than the customer's willingness to pay, the relevant seller "does not capture the full value" of the buyer's purchase. The problem with respect to Internet access is not that the ISPs do not capture the full value of the sale, but that *subscribers* create positive externalities enjoyed by advertisers, information providers, merchants, friends, and acquaintances, and thus subscriber willingness to pay understates the social value created when a new subscriber comes online. [15] Reframed this [*226] way, it becomes clear that this is a standard problem--in many markets there are substantial positive externalities--and that the right response is not a reduction in the incentive to take care. Restaurants, after all, create positive externalities by drawing crowds that in turn patronize neighboring businesses and stimulate the local economy, yet no one suggests that in response local authorities should stop enforcing the health code; that response would just drive customers away. For similar reasons, a reduction in ISP liability is unattractive. As we will explain more fully below, the right response is a tax break or other subsidy that encourages marginal subscribers to stay online even as the costs of service rise.

The second objection is echoed in the preamble to section 230 of the Communications Decency Act, where Congress notes that immunizing ISPs from liability will have the indirect effect of encouraging "the development of technologies which maximize user control over what information is received" [16] and also

"the development and utilization of blocking and filtering techniques" [17] that similarly might empower Internet subscribers to bar unwanted messages. The objection is that allowing ISPs to shirk will increase the incentive for subscribers to engage in self-defense and, through that, the incentive for independent firms to step in and offer technological solutions along the lines of virus protection software and firewalls. That is all true, but, as we will argue below, the logical implication is not complete immunity for ISPs. Instead, liability should be tailored in light of this possibility for market-based self-help, the goal being to encourage service providers to adopt the precautions that they can provide most efficiently while leaving any remaining precautions to other market actors. This is again a standard scenario. Pedestrians can exercise care in crossing the street. They can also stay at home rather than venturing near the roads, and they can wear unfashionably bright attire so as to increase the odds of being seen at night or during inclement weather. Yet these simple facts do not lead anyone to suggest that, because pedestrians can engage in their own forms of precaution, automobile drivers should be immune from tort liability. The same intuitions apply here. The fact that multiple parties can take precautions against malicious computer code might argue for some form of balanced liability regime that leaves both subscribers and ISPs with some incentive [*227] to take care, but that fact does not in any way argue for complete immunity for ISPs. There are precautions in which ISPs can and should engage, and shifting the full costs of cyber-security to Internet subscribers would inefficiently reduce each ISP's incentive to take them.

Now a word on our terminology. We do not need a formal definition of the term "Internet service provider" in order to capture the basic idea that these are the entities that provide individual and institutional subscribers with access to the Internet. The precise features associated with that access are not of concern. Some ISPs offer email services, news, storage space, and even games to their subscribers. Others simply receive data, convert that data into a form consistent with the TCP/IP protocol, and forward the results to independent computers that then provide richer services and interactions. All of these entities, however, are for our purposes considered "Internet service providers" in that each controls the point at which information residing on a privately owned computer network first comes in contact with the public network. Thus--and perhaps these will quickly sound to readers like historical references, given the pace of change in the industry--SBC is an Internet service provider in our vernacular, as is America Online, Road Runner, and RCN.

We similarly see no need to adopt technical definitions for concepts like the computer worm, the computer virus, the denial-of-service attack, or even the software Trojan horse. For us, these serve as mere placeholders for any category of malicious computer code that is propagated on the Internet, using or interfering with privately owned computer equipment, and done in a way such that the relevant private party has not given informed consent for that use or interference. Details beyond that--while certainly relevant to an understanding of the specific steps that might be available to combat pests--have no impact on the legal argument we present.

Our discussion proceeds in five parts. Part II summarizes the conventional economic account of indirect liability and applies those teachings to the specific case of Internet service providers. Part III considers in more detail the two primary objections sketched above, namely: (1) that liable ISPs will be overly cautious and thus inefficiently exclude marginal subscribers; and (2) that liability will reduce user incentives to engage in efficient self-help. Part IV questions several recent court decisions that seem unnecessarily reluctant to hold ISPs accountable for the bad acts of their subscribers. Finally, Part V concludes with some remarks on the limitations of our analysis and how our discussion differs from what might otherwise be a comparable discussion of ISP liability in the context of online copyright infringement.

## [*228] II. THE THEORY OF INDIRECT LIABILITY

### A. The Standard Model

Indirect liability is said to attach in instances where the law holds one party liable because of a wrong committed by another. [18] A familiar setting is the employment relationship, where an employer can be held liable for torts committed on the job by his employees. [19] But other examples abound. Bars are sometimes held liable when bartenders serve alcoholic beverages to patrons who later harm others while driving

under the influence. [20] A motor vehicle owner can be held to account if a driver to whom he loans his car ends up causing an accident. [21] Landlords are sometimes on the hook if they take inadequate precautions against criminal activity that in turn harms tenants. [22] Mall owners can be held responsible if merchants use mall premises to sell counterfeit or gray market goods. [23] Even product liability law has this same basic structure: a buyer might use a dangerous product such as a car in a negligent manner and cause injury to a third party; if the victim can show that the accident would not have occurred had the manufacturer employed a better design, the victim may be able to recover from the manufacturer instead of (or in addition to) the buyer. [24]

[*229] Conventional economic analysis suggests that an explicit rule imposing indirect liability is not necessary when two conditions are simultaneously met: first, the relevant direct actors are subject to the effective reach of the law, by which we mean that the employees, drivers, and merchants discussed in our previous examples are easy to identify and have assets that are sufficient to pay for any harm caused; and, second, transaction costs are such that those direct actors can use contract law to shift responsibility to any party that might otherwise be an attractive target for indirect liability. [25] The intuition is that, when these conditions are satisfied, the various parties can create indirect liability by contract, and--albeit subject to some second-order constraints [26]--will do so where that would be efficient. [27]

To see this, consider the employment setting in more detail. If the driver of a delivery van is himself easy to identify, and, further, the driver has adequate resources to pay for whatever harm he might cause in the event of an accident, then there is no strong argument for imposing liability on the associated retailer. No matter what the legal rule, the driver and the retailer will efficiently allocate liability through their employment contract. Thus, if the optimal rule would impose on the retailer the obligation to inspect every delivery van each morning, or to test employees randomly for drug and alcohol abuse, the driver and retailer will agree by contract to those desired monitoring activities. Similarly, to the extent that driving the truck poses an unavoidable risk of injury to others, the driver will either shift that risk to the employer through an indemnity clause or assume that risk and demand higher wages in compensation. The legal rule in this situation is just a default; where transaction costs are low and employees have adequate resources, contracts allow private parties to shift and divide legal responsibility efficiently.

Things change when either of the conditions identified above fails to hold. For instance, where contracts are easily negotiated between the driver and the retailer, but the driver himself lacks the resources [*230] necessary to pay for the harm he might cause, the absence of indirect liability would tempt the retailer to leave tort liability on the shoulders of the driver, in essence using the driver's financial limitations as a cap on legal liability. Similarly, where contracts are possible but a negligent employee's identity cannot be ascertained--for example, witnesses report that a Federal Express van hit the pedestrian but no one saw the driver--again the absence of indirect liability would act as a *de facto* cap on tort liability, putting the driver in a position where he would not be fully liable for his accidents and thus leading the retailer and driver together to take suboptimal care. Where the driver has adequate resources but the parties cannot contract effectively, the legal rule clearly matters as well, this time because the inability to contract would make it impossible for the parties to shift responsibility to the cheaper cost avoider.

Thus the interesting cases are those where either the relevant bad actors are beyond the reach of the law, or transaction costs make reallocation by contract implausible. For these cases, economic analysis identifies two additional considerations: first, indirect liability might be attractive in cases where one party is in a good position to detect or deter another's bad act; and, second, indirect liability might be attractive in cases where liability would serve to encourage a party to internalize some significant negative externality unavoidably associated with its activities. [28]

Start with the first consideration: that indirect liability might be particularly attractive where the potentially liable party is in a good position to detect and deter bad acts. This is, for example, one of the main reasons why employers are responsible for the torts committed by their employees. An employer can control his employees. He can monitor their behavior, screen them before entrusting them with dangerous equipment, develop compensation schemes that encourage them to exercise due care, and otherwise beneficially influence their on-the-job decisions. The prospect of indirect liability pressures employers to make use of

these mechanisms and in that way to minimize the expected cost of accidents. Now admittedly employer liability is typically strict, which is to say that--despite what we just [*231] said--liability does not turn on a specific court finding that the relevant employer should have taken additional precautions given the particular accident at issue. However, the logic is likely that the more detailed inquiry would prove too cumbersome, and thus the law errs on the side of holding employers accountable. In essence, strict liability in this application presumes that there was something that the employer should have done differently, and that presumption is made irrebuttable for reasons of administrative convenience. In many other settings, by contrast, some form of a negligence standard is used, and that maps well to the intuition that the liable party had the ability to control the erstwhile bad actor and inefficiently failed to do so. [29]

Turn now to the second factor: that even in situations where the indirectly liable party cannot meaningfully detect or deter bad acts, indirect liability might still be attractive as a means by which to force that party to account for significant negative externalities unavoidably associated with its activities. Again, the employment setting is instructive. Even where a retailer can do nothing more to ensure that the drivers of its delivery vans take appropriate care, it is likely efficient to have the retailer pay at least some fraction of the costs of any delivery accidents. The reason is that this forces the retailer to account for the costs of accidents when deciding the price and frequency of deliveries. If accidents are unavoidable, liability means that price will rise and quantity will fall, which is exactly what should happen given this unavoidable harm. This is referred to in the literature as an effect on "activity level," the vocabulary there designed to emphasize that the purpose of liability here is not to encourage precautions but instead to influence how often the harmful activity in question takes place. Importantly, note that where activity level is the concern, strict liability is often appropriate, in that the logic of liability is not at all tied to any negligent failure on the part of the indirectly liable party to take some cost-justified precaution.

These factors--call them "control" and "activity level"--help to identify cases where liability might be attractive. The actual question of whether liability should be imposed, however, typically turns on other, often setting-specific, considerations. Thus, while the telephone company surely has the ability to deter crank phone calls by more carefully monitoring calling patterns, it is unlikely that telephone company liability would be attractive, both because of obvious privacy concerns and because of worries that, in its attempts to address the problem of crank calls, the telephone company would inadvertently interfere with substantial legitimate telephone activity. To [*232] reject indirect liability in this situation is in essence to announce that the costs of crank telephone calls are not sufficiently high as compared to the costs of indirect prevention. Similarly, the mere fact that an airport provides a venue from which airlines generate pollution and noise does not itself justify imposing liability for those harms. After all, private parties who own property near the airport themselves make decisions that increase and decrease the importance of airport externalities. In a world where the airport absorbed these costs in full, neighbors might inefficiently decide to use their properties to raise livestock or care for the elderly, two uses so sensitive to noise and pollution that they likely should be disfavored given the proximity of the airport.

That said, the control and activity-level considerations do helpfully sketch the contours of efficient indirect liability rules. For instance, these factors make clear why employers should not typically be held accountable for torts committed by their employees in instances where the employees are acting outside the scope of employment. The employer has no special advantage when it comes to stopping employees from abusing their spouses or picking fights at bars. [30] Moreover, neither activity is rightly understood as a consequence of the employer engaging in whatever its core business might be; whether the employer is in its current line of business or another, the employee is probably just as likely to commit these bad acts. Thus, except in exceptional circumstances, neither the control nor the activity-level rationale fits, and liability for torts committed outside the scope of employment is therefore inappropriate. [31]

To take another example, an efficient indirect liability regime should be reluctant to wave off liability in cases where the potentially liable party asserts, as a defense, that he lacked control over the alleged bad actor due to a contractual provision, an affirmative technology choice, or some detail related to corporate structure. The idea [*233] behind the control rationale is to encourage private parties to develop mechanisms and adopt organizational structures that effectively allow for the control of possible bad actors. Allowing parties to hide from this obligation through some voluntary limitation threatens to

undermine that logic, in essence encouraging a potentially liable party to knowingly and intentionally stick his head in the sand. Sadly, courts accept these sorts of excuses all too often--this is exactly the ruse at play in situations where taxi cab companies structure their affairs such that each taxi is, in the eyes of the law, a separate corporate entity [32]--but the basic economics of indirect liability reminds us that courts should instead direct a skeptical eye toward any party's self-imposed inability to detect or deter. [33]

In sum, the conventional economic account makes clear that private parties cannot create the optimal liability regime on their own in instances where the party directly responsible for the bad act is beyond the effective reach of the law, and private parties also cannot create the optimal liability regime on their own in instances where transaction costs make contract negotiations implausible. The conventional account further stresses that liability should be considered in instances where one party has the ability to deter or detect the bad acts of another, and also where liability can serve to encourage a party to internalize some significant negative externality associated with its activities. As we will argue in the next section, violations of cyber-security take place in a setting where these conditions all seem likely to hold.

### B. Applied to Internet Service Providers

There are strong arguments in favor of imposing liability on ISPs for violations of cyber-security, and they track the four core intuitions outlined in the previous section. Consider each in turn.

#### 1. Beyond the Law's Reach

Individuals who originate malicious computer code are typically far beyond the reach of conventional law. For one thing, they are hard to [*234] identify. Sophisticated saboteurs use the Internet's topology to conceal their tracks by routing messages through a convoluted path that is difficult for authorities to uncover. Moreover, by the time a computer virus or worm is detected, the trail often is cold. Internet pests like worms and viruses are routinely programmed to sit idle for a period of time before triggering, which primarily allows mischief-makers to time their attacks to coincide with important world moments--the W32/Mypics virus was designed to launch at the start of the new millennium, for example [34]--but also creates a period of time during which the mischief-makers can effectively disappear. The fact that many hackers reside overseas only exacerbates the problem, introducing issues of jurisdiction and the need for international cooperation.

Even if caught, individuals who create malicious computer code rarely have sufficient assets to pay for the losses they impose. Some estimates put the costs of prominent Internet worms and viruses in the billions of dollars, [35] and those estimates might undercount the harm as they measure only commercial productivity losses and disruptions to commerce, thus ignoring the costs of countermeasures like antivirus software as well as less quantifiable harms such as missed opportunities for communication and the frustration experienced by computer users who are victimized. Obviously, hackers will rarely have resources sufficient to pay up. Criminal liability could, in theory, substitute as a deterrent; however, where the risk of apprehension is sufficiently small and the magnitude of the loss sufficiently large, criminal punishments often cannot be made high enough to adequately deter. Judges may be reluctant to impose too large a sentence for nonviolent crime, and, besides, long-term incarceration is expensive to the state. [36]

Interestingly, concerns about bad actors being beyond the reach of the law do not apply to the individuals and entities who, instead of creating an Internet pest, inadvertently propagate one. An example [*235] might be a firm whose server is run in such a way that an outside party can easily take it over, or an unsophisticated Internet user who installs a malicious program when prompted to do so by an anonymous email solicitation. There is no reason to believe that careless firms and unsophisticated users lack the resources necessary to pay for whatever harm they cause. Moreover, careless firms and unsophisticated users would typically not be that hard to track down. Computer users who fail to exercise appropriate caution when opening email attachments, for example, are hardly likely to be sophisticated enough to cover their tracks in the event of a problem. The only sense in which these bad actors are beyond the reach of the law is the practical concern about the costs of identifying and suing them as compared to the fraction of the damages for which they might be held legally responsible. Beyond that, parties who

propagate but do not create malicious code are not beyond the reach of the law; although, as will become clear below, there are other reasons why indirect liability might be warranted even in these sorts of cases.

### 2. Contracts and Transaction Costs

A second consideration raised in our baseline analysis concerned the ability of the relevant parties to allocate liability by contract. We are not here referring to the contract that a given subscriber might sign with his chosen ISP. Obviously, such contracts exist, and through their various terms of service those contracts do in fact allocate liability between each ISP and its subscribers. Our focus is instead on contracts that would obligate an ISP to protect other ISPs from any harm caused by the first ISP's subscribers. Our point is that ISPs in theory can use contract law to create this sort of system-wide liability. That immediately raises the question of why those obligations are not in place, and whether the law should respond by imposing them.

An intuitive answer is that there are today so many ISPs in operation that the transaction costs of negotiating the necessary web of contracts would be prohibitive. But that explanation is only marginally satisfying, in that ISPs are already all part of a complicated and fully inclusive network of contracts, specifically the "peering" and "transmit" agreements under which the various private owners of the Internet backbone agree to carry traffic one to another. [37] A more satisfying explanation is that any network of contracts focusing on issues of cyber-security would be perpetually out of date, and updating [*236] such a complicated web of interdependent security obligations would be all but impossible given the number of parties involved and the complicated questions any update would raise regarding appropriate adjustments to the flow of payments. [38]

Still, there are puzzles lurking. Microsoft has licensing agreements with a huge percentage of home computer users, and thus the firm seems to be in the perfect position to ensure that users take sensible precautions like updating their virus software and downloading system patches. Microsoft could even make those obligations self-executing by blocking Internet access for any computer whose software is (say) more than 10 days out of date. Instead, Microsoft merely offers updates to its customers and allows each customer to decide whether the private benefits of a given update warrant the private costs in terms of time and inconvenience. The result might very well be a classic case of externalities leading to suboptimal behavior: Microsoft's customers as a group would be better off were each to update regularly, but, without coordination, each customer opts to update less frequently. This suggests that there must be a bigger problem with contractual solutions--public relations? privacy concerns? security? [39]--although in truth the explanation might simply be that Microsoft is at the moment in too precarious a position vis-a-vis worldwide antitrust authorities to do anything that might be perceived as the use of its market power to foist additional software on unwilling consumers.

### 3. Control

As we noted in the more general discussion, indirect liability is primarily attractive in cases where the indirectly liable party can detect, deter, or otherwise influence the bad acts in question. ISPs seem to be a natural choice under this criterion. Consider, for example, an ISP through which a troublemaking user obtains access to the Internet. Such an ISP can detect criminal behavior by analyzing patterns of use, much as a bank can detect credit card theft by monitoring each [*237] customer's pattern of purchases. Easiest to catch would be patterns that are intrinsically suspicious, such as a continuous stream of communications from a home user or the repeated appearance of identical computer code attached to a large number of outgoing email messages. But an ISP could also detect patterns that are suspicious because they represent a radical departure from the user's ordinary behavior. The ISP would need only maintain a profile that captures in broad strokes each subscriber's rough practices and then evaluate recent activity against that historical backdrop. Again, credit card companies actually do this, and ISPs could do it too.

Another option might be to record a subscriber's data stream and store that information, ideally in encrypted form, for a period of time. Many offenders could be traced if ISPs were to record traffic in this

manner. But ISPs do not routinely record traffic today, both because of privacy worries and because of the enormous volume of communications. Legal rules, however, could ease those concerns. For instance, the law could require that ISPs store the information securely and release it only to law enforcement officials, thus lessening the worry that stored information would leak out by accident or be used for impermissible purposes. The law could also require that ISPs record information about the data communication--size, duration, timing, and so on--but not its substance, thus protecting privacy and reducing volume. The law could even require ISPs to record information only when particular triggers raise suspicion, or perhaps only in response to specific government requests. [40] The amount of time that information would need to be stored could also be tweaked to address concerns about storage costs, assuming those concerns are valid and not a pretext advanced by ISPs to avoid regulation.

We have focused thus far on bad acts engaged in by a subscriber or accomplished using a subscriber's account, but turn now to the role ISPs might play in detecting criminal behavior that originates on a rival firm's network. When an ISP receives a packet or message from another ISP, it might be able to detect aspects of the packet that indicate [*238] a likelihood of criminal activity. For example, an ISP might alone, or in cooperation with other ISPs, notice an unusual spike in demand, indicating a denial-of-service attack or a rapidly multiplying virus or worm. ISPs might even be able to develop efficient protocols for pooling information about changes in traffic patterns and in that way alert one another, and also customers, of suspicious behavior in time to trace it back to its source or at least to shut it down before it can cause substantial harm.

We could go on for some time with examples along these lines. However, our goal for now is not to determine the precise precautions that ISPs should or will take in response to liability--quite the opposite, we are painfully aware of our outsider status when it comes to technology design--but instead to make clear that ISPs are in a good position to influence the number and severity of cyber-attacks. Indirect liability would pressure service providers to take this task seriously, ensuring that those who have the proper technical expertise will themselves work to identify and then implement whatever turn out to be the most effective precautions.

**4. Activity Level**

In theory, indirect liability can be attractive independent of its role in encouraging detection and deterrence because liability encourages a party to account for any negative externalities unavoidably associated with its product or service. In practice, however, we doubt that we would favor ISP liability on this argument alone. Our hesitation does not derive from any doubts over whether ISPs impose negative externalities as they enroll new customers and offer new services; of course they do, given that any new subscriber can turn out to be a careless user, and any new service can quickly devolve into a portal for Internet contagion. Our hesitation instead derives from the fact that there are drawbacks to imposing liability solely because of negative externalities, and those drawbacks are significant in this particular application.

One drawback associated with the activity-level rationale is that it might distort behavior by forcing parties to internalize negative externalities even though they often cannot internalize equally sizable positive externalities. As applied here, the negative externality is the aforementioned concern that each new subscriber could materially reduce cyber-security by engaging in unsafe practices or intentionally introducing an Internet pest. [41] The comparable positive externality is that each subscriber can just as plausibly turn out to be a homemaker [*239] who makes significant purchases online or a college student who posts to newsgroups and contributes to the development of open source software. Liability that encourages ISPs to take precautions is one thing, but a legal rule that relentlessly brings home negative externalities while completely failing to account for positive externalities has no claim at creating optimal incentives. Thus, a rule that imposes liability based on negative externalities might do more harm than good--although the actual analysis turns on the relative size of any ignored positive externalities and the difficulty of accounting for those externalities through other means. We will say more about that below.

A second drawback to the activity-level rationale--and on this, too, we will say much more below--is the

concern that imposing liability on one party almost inevitably discourages another party from taking adequate precautions. Applied here, the worry is that imposing liability on ISPs might inefficiently reduce subscriber incentives to install virus protection software and to maintain adequate firewalls and backups. This is a concern associated with indirect liability no matter what the rationale; but the concern resonates with particular force in cases where indirect liability is being used solely as a means by which to influence the liable party's activity level. The reason: these are cases where by assumption the liable party cannot take additional cost-justified precautions; reductions in the level of care taken by other parties therefore warrant considerable weight.

A third argument against imposing strict liability solely because of activity-level concerns is that activity levels in this setting are already significantly suppressed. Worms, viruses, and the like reduce the allure of Internet access and thus discourage Internet use no matter what the liability rule. This is a natural reduction in activity levels, and--while there is no reason to believe that it leads to efficient levels of activity [42]- the existence of this natural disincentive does combine with the concerns discussed earlier to make any additional reduction seem not only less important, but also more difficult to calibrate.

All that said, activity-level concerns can be important, and hence we do harbor some uncertainty over where to draw this line. Consider [*240] again Microsoft. Even if Microsoft cannot take additional precautions against Internet contagion, the price increase that would likely result from an increase in liability would itself have social benefits in that the resulting price would better reflect the relative value of the Windows operating system as compared to alternatives like Apple Computer's operating system, Mac OS. Many computer enthusiasts believe that Mac OS is more stable and secure than Windows. If so, this benefit is not today adequately captured in the products' relative prices. By increasing liability and hence disproportionately increasing the price of Windows software, however, an indirect liability rule could help to solve that problem, ultimately driving business toward the more secure and efficient alternative.

More generally, in situations where several competing products are each capable of generating a comparable positive externality, it might be attractive to use indirect liability as a way of pressuring firms to select prices that accurately reflect each product's unique negative externalities. Suppose, for example, that ISP access provided over the telephone lines using DSL technology is worse, from a cyber-security standpoint, than ISP access provided using the cable infrastructure. If true, and even if providers of those technologies cannot take any additional cost-justified precautions, liability might be attractive. All else held equal, the technology that imposes the greater security risks would under a liability regime cost more, and the resulting price difference would drive customers to the socially preferred technology. [43]

## III. OBJECTIONS

Our argument thus far is that indirect liability is attractive primarily because ISPs are in a good position to deter the various bad acts associated with cyber-insecurity, and perhaps secondarily because liability would force ISPs to internalize some of the negative externalities they impose. Further, we have argued that any indirect liability regime needs to be created by law, rather than by contract, both because many of the relevant direct bad actors are beyond the reach of law, and because transactions costs are a serious obstacle to contractual solutions in any event. We turn now to what we anticipate to be the primary objections to our analysis: first, that liability will cause ISPs to overreact and thus exclude subscribers who should be online; and, second, that liability will inefficiently interfere with subscriber efforts at self-help.

### [*241] A. Overzealous ISPs

The most common objection to ISP liability is that it will deter ISPs from offering service to innocent but risky users. Phrased in the more formal language of economics, the concern is that a positive externality is created every time a new user subscribes to Internet service, and thus, if Internet access is priced at marginal cost, some subscribers will not purchase Internet access even in situations where the social benefits of access exceed the social costs. [44] More intuitively, indirect liability will inevitably raise the price of service because of the added costs and legal exposure, and, while that higher price might better

represent the real costs associated with Internet access, it will also drive some marginal subscribers out of the market despite the fact that advertisers, information providers, merchants, friends, and various other subscribers might in the aggregate prefer that these marginal customers remain. The problem is just an externality--a mismatch between the private incentive to subscribe to Internet service and the social benefits made possible by that same subscription.

Our first response is that this concern, while plausible, seems overdrawn. Many of what at first sound like externalities turn out to be influences that are already accounted for in a subscriber's decision whether to subscribe. For instance, Lichtman certainly benefits from the fact that his mother is regularly online and hence available for easy email correspondence, but that is not an externality because Lichtman and his mom have a rich relationship through which he can indicate to her how much he values her presence and, if necessary, contribute in cash or kind toward the monthly costs of her subscription. So, too, the online bookseller Amazon.com benefits from Mom's Internet access, but Amazon also has ways of helping her to internalize that effect, for instance by rewarding her with free shipping on her purchases. This is obviously not to say that all externalities are internalized, but only to suggest that the problem is not as stark as it might at first seem, and not all that different from a million other markets where incidental positive externalities slip through the decision-making cracks. [45]

[*242] Second, even if there are nontrivial positive externalities at play, note that it would be counterproductive to respond to the problem by reducing ISP liability from its otherwise optimal level. Simply put, if the concern here is that higher prices will force marginal subscribers to leave the market, the reality is that an increase in worm and virus activity will also drive away marginal subscribers. That is, cyber-insecurity, like an increase in price, is a cost associated with online access; it, too, will make Internet access less attractive to private parties, and thus it too threatens to inefficiently drive away customers whose private benefits fall short.

Now the choice between these evils is itself an interesting question. One might at first suspect that indirect liability produces the better form of exclusion because ISPs will channel that exclusion such that it affects more significantly those users who are perceived to pose the greatest likelihood of harm. Thus, a user whose actions online reveal him to be a risky user will be charged a higher price by his ISP, whereas a user who credibly signals safety will be charged a correspondingly lower fee. The economic effect is that indirect liability should disproportionately exclude those subscribers who are in fact the least desirable subscribers. The exclusion caused by worms and viruses, by contrast, lacks such nuance. A denial-of-service attack can slow even the most responsible user's machine to a crawl, and viruses that interfere with the delivery of e-mail messages likewise disrupt communication for every user. Then again, Internet pests impose greater costs on careless users than they do on careful ones; a user who regularly updates his virus software and backs up his files has less to fear from Internet contagion, because his computer will more likely be resistant. But this argument does not apply to malicious users who intentionally contaminate the network, and because of them it seems likely that the targeted exclusion caused by indirect liability is more appealing than the less focused exclusions caused by worms and viruses.

Regardless, there is no reason to choose from among these second-best alternatives, as quickly becomes apparent when one switches attention away from Internet access and toward more conventional legal settings. Inventors produce devices that stimulate further innovation. In response, society rewards them by granting them valuable property rights called patents. Does anyone really believe that society [*243] should instead shield inventors from liability if their inventions cause harm? Similarly, restaurants draw crowds that patronize neighboring businesses and stimulate the local economy. Local authorities therefore sometimes offer tax breaks to restaurants that are willing to locate in depressed neighborhoods. Would it be desirable to instead entice entry by offering to stop inspecting for violations of the health code? People who generate positive externalities are not typically compensated by legal immunity. Quite the opposite, even an entity that produces positive externalities should still take due care while engaged in its beneficial activities. There is nothing special in this respect about the Internet. Immunizing ISPs from liability is not the correct mechanism for encouraging them to provide positive externalities.

We see two better approaches. One is to subsidize the provision of Internet access, for example by offering tax incentives to ISPs based on the size of their subscriber base. The government today already subsidizes Internet access by providing a great deal of the equipment that makes up the Internet backbone, and also by forbidding states from collecting sales tax on large categories of otherwise taxable Internet transactions. [46] Those existing subsidies alone might be sufficient; [47] but, if necessary, the government can do more. For instance, in the context of the regular voice telephone system, the federal government subsidizes the purchase of local telephone service both through specific programs designed to assist poor and rural subscribers, and through more general pricing policies that favor residential users over commercial ones. [48] The logic there is similar to the logic under consideration here; the telephone system is just another network out of which individuals might inefficiently opt but for the appropriate government subsidy.

A second approach would have the government work with ISPs to redesign Internet protocols so that ISPs could more precisely charge one another for transferring information. [49] Under the current system, when a new user joins the network, neither that user nor his ISP captures the full benefits associated with the new subscription. However, [*244] if ISPs could charge one another for relaying messages back and forth, and then in turn pass those costs and payments along to their customers, each ISP would internalize the benefits of adding a new user and thus each would better weigh the benefits as well as the costs every time it confronted the question of what price to charge for access.

**B. Subscriber Self-Help**

It is true that, by imposing liability on ISPs, our approach would reduce subscriber incentives to practice safe computing, install firewalls and virus protection software, and similarly engage in prudent self-help. This is troubling because subscribers are often in a better position than their ISP to determine that their computers have been hacked; and, relatedly, users are often themselves in a good position to take simple, inexpensive, but effective precautions like using appropriate passwords in order to prevent unauthorized use in the first place. Furthermore, when subscribers are looking to protect their computers from cyber-mischief, the competitive market responds with third-party software and technology; that market might not be as active in a world where subscribers are uninterested and thus the only buyers are regulated telephone companies and other entities that provide Internet infrastructure. [50]

It is important, however, not to overstate these tensions. ISPs have a direct contractual relationship with their subscribers, and so surely a liable ISP will require that each of its subscribers adopt rudimentary precautions along the lines sketched above. Better still, those contract terms can be enforced by technology, which is to say that an ISP can block any subscriber whose virus definitions are horribly out of date or whose firewall is malfunctioning. Even outside of any contractual obligations, it is typically in a subscriber's own interest to protect his computer, at least to the extent that precautions are not too cumbersome. In fact, one suspects that the real obstacle to self-protection at the moment is merely a lack of information. Were ISPs to better explain to users exactly how to minimize their exposure, many users would happily cooperate, wanting to protect their personal documents, digital music, and family photos from contamination and irreversible loss.

[*245] All that to one side, our main response to this concern about reduced incentives to engage in self-help is that, even at its strongest, this effect does not argue against indirect liability writ large but instead simply suggests a need for a tailored threshold of liability that would pressure subscribers to take adequate care. This is just like the airline example where the conventional wisdom argues against holding airports strictly liable for pollution and noise externalities, the fear being that neighbors would then ignore those factors when deciding how best to use nearby properties. The fact that multiple parties can take precautions against malicious computer code does not in any way argue for complete immunity for ISPs. There are precautions in which ISPs can and should engage, and shifting the full costs of accidents to Internet subscribers would inefficiently reduce each ISP's incentive to do so.

On this same theme, note that nothing that we say about indirect liability for ISPs is meant to suggest that Internet subscribers should themselves be immunized from liability. Many users have deep

pockets--businesses and universities, for example--and making them liable for cyber-mischief will create additional incentives to take precautions. Liability would also create a beneficial cascade in which these businesses and universities would then work to prevent employees, students, and the like from similarly engaging in intentional bad acts or adopting inadequate security precautions. The general insight, then, is that neither users nor ISPs should be given a complete pass when it comes to cyber-security. Each has a role to play, and each should therefore be held accountable at least in part.

### C. Other Objections

While the previous sections consider the two primary objections to ISP liability, there are of course other issues to address. We survey a few of those below.

One problem with ISP liability is that often the harm will be spread so thin that no victim in isolation will have a sufficient incentive to bring suit. An example might be a situation where a user launches a worm that slows down the Internet somewhat, resulting in some delays and loss of business, but does not harm any individual or business very much. This is a classic case of diffuse harm, similar to pollution that bothers many people but not enough to motivate litigation. There are two standard solutions to this problem. First, entrepreneurial lawyers might combine all the victims into a single class and sue on behalf of the class. Attorney fees give the lawyers an incentive to launch the lawsuit. Second, the government--through assistant attorneys general or an appropriate agency such as the Federal [*246] Trade Commission--could bring the lawsuit. There are advantages and disadvantages to these approaches, but those arguments are well known and hence we will not repeat them. [51]

A related problem concerns allocation of liability across ISPs. A communication that originates a virus, for example, might pass through dozens or hundreds or thousands of ISPs before claiming its first victim. Suppose any one of them could have detected the virus; should liability be allocated such that each ISP pays only its pro rata share? Certainly one good answer here is joint and several liability, which allows victims to sue any of the liable ISPs for the entire harm. The chosen ISP could then pass along some of the expense to its culpable peers. In this way joint and several liability lowers the barrier to litigation as faced by the injured party. Rather than having to identify and sue all the relevant ISPs, the victim can sue the easiest target and leave any division up to litigation between, and perhaps contracts among, the various ISPs.

An additional worry related to ISP liability is the possibility that imposing liability will have perverse effects, for example encouraging ISPs to store less information and in that way make effective legal intervention more difficult. [52] These sorts of concerns can be addressed either by the procedures for proving liability or its substance. Thinking first about the standard. If the burden of proof is placed on the ISP to prove adequate precautions, these sorts of strategic responses become less attractive from the ISP's perspective. With respect to the substance, meanwhile, the decision not to keep adequate information could itself be deemed actionable, thus more explicitly encouraging ISPs not to strategically destroy information. All this is fully consistent with our earlier remarks concerning employer/employee liability; as we pointed out there, employers are typically held strictly liable for the torts of their employees, in part because the more careful inquiry into exactly what precautions were and should have been taken is also subject to these sorts of informational games. [53]

A final objection to ISP liability is the familiar concern that any domestic legal regime will have only a limited effect because of the problem of foreign ISPs. Suppose that the U.S. adopts the optimal ISP liability regime, with one result being that any major cyber-crime originating with an American ISP can be traced back to its source. According to this argument, American Internet users would nevertheless [*247] remain vulnerable to foreign criminals who launch attacks from computers in countries with weaker Internet regulation, and to American criminals who are able to hide their identities by routing incriminating packets through those same foreign ISPs. Imposing liability might therefore seem to be an empty gesture, merely shifting criminal behavior from one ISP to another.

The problem is acute because of the "weakest-link" nature of the Internet. There are roughly 200 states;

suppose that 199 of them have the optimal Internet security system. The other state--call it Estonia--has no regulation. The ISPs there keep no records, so law enforcement authorities cannot trace cyber-crimes to particular users. Not only can criminals in our hypothetical Estonia therefore launch untraceable attacks on users anywhere in the world, criminals in the 199 other countries can launch untraceable attacks on users anywhere in the world by routing their messages through Estonian ISPs. Worse, authorities in, say, Canada cannot solve this problem by refusing to allow packets that pass through Estonia to cross Canadian borders because (absent a massive change to the architecture of the Internet) there is no way for a Canadian ISP to determine whether a packet it receives ever passed through an ISP located in Estonia, unless it receives that packet directly from an Estonian ISP rather than an ISP in a third country. Thus, as long as there is one state with bad regulations--and currently there are dozens of states with bad regulations--cyber-crime, including purely domestic cyber-crime routed through foreign ISPs, will be difficult to trace and stop.

However, even in a world where foreign rules offer little assistance and it is relatively easy for cyber-criminals to take advantage of the weakest state's rules--and one might wonder whether those statements are true, given how often cyber-criminals are being arrested abroad [54]--domestic regulations can still reduce the likelihood that any given pest will propagate. Indeed, as we have pointed out before, domestic ISPs can detect disturbing patterns in the packets they receive from other sources, they can pressure subscribers to adopt appropriate security precautions, and they can themselves adopt policies that mitigate the harm caused by worms, viruses, and the like. Weak foreign regimes therefore might interfere with some of the deterrence effect that would otherwise be achieved by the optimal ISP regime, but it certainly does not fully eliminate an ISP's ability to adopt effective precautionary techniques.

Moreover, one country's rules can and certainly do influence the [*248] rules adopted by economic and political partners. Thus, if the United States were to adopt a more stringent set of ISP regulations, it could pressure allies and trading partners to adopt a similarly forceful regime. It might do so using the normal tools of international diplomacy--adjusting terms of trade, offering an economic or political quid pro quo, and so on--or it might do so by adjusting the rules that govern the flow of Internet traffic. [55] For instance, suppose that the United States and a few other core states such as Japan, the European Union nations, and Canada were to enter into an agreement requiring each state to exclude Internet packets from (1) all states that have bad Internet regulation and (2) all states with good Internet regulation that do not exclude packets from states with bad Internet regulation. With a core group signed onto such an agreement, a state like China would face the choice between adopting the required Internet policies and enjoying free communication with its main trading partners, or persisting with a less secure regime but no longer being able to communicate over the Internet with member countries. China, we suspect, would choose the former option, and that would in turn put more pressure on the next outlier nation to capitulate as well. As more states made this decision and entered the secure bubble, the opportunity cost of remaining outside the bubble would increase, and eventually a healthy percentage of the world's states would be working within a more secure Internet architecture.

## IV. RECENT CASES

We have argued thus far that Internet service providers should be held liable for a variety of cyber-security harms; yet recent trends in the law have pressed in the opposite direction. The trend in the legislature we mentioned at the outset: the Communications Decency Act of 1996 and the Digital Millennium Copyright Act of 1998 immunize ISPs from liability that common law principles would otherwise impose. The trend in the courts looks no better. One recent decision, for example, reads the Communications Decency Act to provide immunity even in settings where the "communication" at issue is not a [*249] defamatory statement but rather a snippet of malicious computer code. Another questions ISP liability more broadly, asking whether ISPs should ever be held liable for harms imposed on "strangers"--that is, Internet users who connect using an ISP other than the one accused of failing to take adequate care. These and related decisions are troubling from our perspective, as they stand as an obstacle to the legal rules we think appropriate.

In this final section of the essay, we therefore set out to consider several of these decisions in fuller detail.

We should make clear before doing so that we do not have strong priors about whether ISP liability should be imposed via federal statute or, instead, through the more gradual mechanism of common law development. There are advantages and disadvantages to both approaches, and in the end much turns on which approach better gathers, communicates, and updates information about ISP capabilities. Our purpose, then, is not to weigh in on that particular tradeoff, but instead to address some of the stumbling blocks that have unnecessarily and prematurely derailed that worthwhile inquiry. Our position is that one should not read the Communications Decency Act to sweepingly preempt state and common law liability for ISPs; and, likewise, one should not interpret the common law such that ISPs have no duty to exercise care in the first place. Beyond that, we understand that reasonable minds might disagree about the precise mechanisms for and contours of ISP liability, and we simply urge that some form of liability be brought to bear.

**A. The Communications Decency Act**

In cases involving business disparagement, defamation, and related state and common law wrongs, the standard legal approach has been to hold speakers and publishers liable for the communications they put forward, but to immunize booksellers, libraries, and similar "distributors" so long as they neither knew, nor had reason to know, of the underlying bad act. [56] Thus, if an article in *Time* magazine is found to impermissibly besmirch an individual's reputation, the writer might be held accountable for defamation, and the publisher might be required [*250] to pay damages, but, barring exceptional circumstances, shops that sell the magazine and libraries that lend it face no legal exposure.

Before the Communications Decency Act was enacted, courts endeavored to apply this liability framework to ISPs. Thus, in *Cubby v. Compuserve,* [57] the court refused to hold an early ISP accountable for defamatory statements communicated through its equipment, primarily because the relevant ISP was, in the court's view, a passive distributor of that information rather than its active publisher. "A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor than that applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information." [58] Soon after came *Stratton Oakmont v. Prodigy Services,* [59] where on similar facts a different court determined that the relevant ISP was more appropriately characterized as a publisher. "By actively utilizing technology and manpower to delete notes from its computer bulletin boards . . . [this ISP] is clearly making decisions as to content, and such decisions constitute editorial control." [60] Other courts similarly worked to select the appropriate analogy based on the facts of the dispute at hand, with the result in each case being heavily influenced by the accused ISP's own choices with respect to its usage policies, its enforcement practices, and its technologies.

This gradual development of touchstones and distinctions might have continued for some time but for a simple and predictable problem: the liability rules were discouraging ISPs from attempting to filter problematic communications. After all, an ISP that refused to self-regulate was likely to fall under the *Cubby* analysis and be characterized as a passive, and hence virtually immune, distributor. An ISP that endeavored to filter, by contrast, was vulnerable to the *Stratton Oakmont* line of reasoning and its associated legal risks. The result was that, because ISPs were so flexible in terms of the precise role they could play in online communication, the standard liability framework created a perverse incentive to sit idly by without even attempting to detect and deter bad acts. [61] That strange state of affairs led Congress to revamp the ISP liability regime by enacting the Communications Decency Act of 1996.

[*251] For our purposes, the key provision is section 230, which states that an ISP will not be "treated as the publisher or speaker of any information" provided by a subscriber or other information source. [62] Debates over the proper interpretation of this clause rage, and along two distinct dimensions. First, does the provision fully immunize ISPs from liability for defamation and related wrongs, or does it leave open the possibility that an ISP can be held liable as a "distributor" even if not liable as a "publisher" or "speaker" per se? Second, does the word "information" include only communications that would otherwise be regulated under defamation and similar tort theories--legal rules that obviously implicate serious First Amendment concerns--or does it expand to include any data transmitted by an ISP, including

the various forms of malicious computer code of interest here? Courts have answered these questions so as to preempt all forms of ISP liability and, further, to apply that immunity to all forms of information; but those readings are flawed, in our view, in that they interpret the statute far too broadly.

On the first question, the leading case is *Zeran v. America Online,* [63] where a panel on the Fourth Circuit held that section 230 "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service," irrespective of whether the ISP in forwarding that information acted as publisher, distributor, or both. [64] Speaking to the distinction between publishers and distributors, the court held that by its express terms section 230 immunizes both types of disseminator, because, in this court's view, distributors are just a type of publisher anyway. As the court put it, distributor liability is "merely a subset, or a species, of publisher liability, and is therefore also foreclosed by ? 230." [65] "Even distributors are considered to be publishers for purposes of defamation law." [66]

The court bolstered its analysis with policy arguments regarding an issue we addressed earlier in this Essay, namely the concern that distributor liability would lead ISPs to be overzealous in their filtering of online communications.

> If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement--from any party, concerning any message. Each notification would require a careful [*252] yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. Thus, like [publisher] liability, [distributor liability] has a chilling effect on the freedom of Internet speech. [67]

We will not here address issues of statutory construction and legislative history; those issues are important to the *Zeran* decision to be sure, but they have been analyzed in great depth by others, [68] and they are as of this writing under active review in the courts. [69] We therefore want to focus instead on the policy argument excerpted above and point out that it, too, is suspect. As a general matter, we have already discussed the limitations associated with arguments about overzealous ISPs. Our points were that market forces will largely discipline this sort of behavior and that, to the extent that any significant externalities remain, tort immunity is not an efficient response. But note that the *Zeran* court makes an additional mistake when it assumes that a mere accusation would be sufficient to trigger [*253] ISP liability. In a more familiar setting, that sounds absurd. Would a court really hold a large bookseller accountable for defamation solely because a random patron informed the cashier that a particular title contained an unlawful communication? Of course not. Tort law requires only that a distributor take reasonable precautions. As applied to ISPs, that likely means that an ISP would not be required to do anything in cases where the only warning was an isolated accusation; a serious response would be required only upon a greater showing, such as the sort of detailed showing that the Digital Millennium Copyright Act requires before the protections and obligations of that statute are triggered. [70]

On the second looming interpretive question--whether the word "information" as used in section 230 includes only those communications that would otherwise be regulated under defamation and similar expressive tort theories or instead expands to include the various forms of malicious computer code of interest to us--we have found only one case. In *Green v. America Online,* [71] a subscriber (a man named John Green) claimed that another user sent him a malicious program through a chat room. In the words of

the court:

> Green alleges that John Doe 1 "sent a punter through [Green's ISP, America Online (AOL)], which caused Green's computer to lock up and Green had to restart his computer." Green's complaint describes a "punter" as a computer program created by a hacker whose purpose is to halt and disrupt another computer. . . . Green alleges that he lost five hours of work restarting his computer, causing him damages of approximately $ 400. [72]

Green apparently asked AOL to take action against the unidentified hacker, but AOL refused to do so. Green sued AOL for negligently failing to "police its services." [73]

The court held that Green's tort claim was barred. First, citing *Zeran,* the court neglected the distinction between publisher-style strict liability and distributor-style negligence liability, announcing simply that holding AOL liable for negligence would impermissibly treat AOL as a speaker or publisher. Then, the court applied this [*254] expanded immunity to the facts at hand, reasoning that John Doe 1 is an information content provider, and AOL must therefore be immune from any form of liability thanks to section 230. Green had argued that John Doe 1 is not an information content provider because Doe sent a malicious computer program rather than any intelligible "information." But the court rejected that argument, noting that the dictionary definition of "information" includes any "signal," and a computer program sent through the Internet is just a collection of encoded signals. [74] In short, the court concluded that malicious code is "information," John Doe I is an "information content provider," section 230 applies to all tort claims involving third-party information, and thus AOL is not liable.

This reasoning is dubious. In terms of the statute, the word "information" is ambiguous: it could include any set of signals that is not random noise, or it could be limited to signals that are used to communicate with humans. More importantly, the concern that motivated section 230 was the worry that, as a practical matter, ISPs cannot control or police defamatory content without violating the privacy of their users and chilling legitimate discussion. But that concern does not extend to situations like the one presented here. Judgments about defamation are unavoidably subjective and context-specific, a reality that makes it all but impossible for ISPs to detect and hence deter that bad act. A computer program that shuts down a target computer, by contrast, can be more readily and less intrusively identified. Besides, the social costs of a system where a few innocent programs are accidentally delayed by an overly cautious ISP seem much less onerous than the social costs associated with an equivalently imperfect filter that might interfere with socially important free speech.

Given all this, we urge courts to reject the analysis of *Green v. America Online* and instead to interpret section 230 such that its immunity extends to "information" that is intelligible to human beings--either in the raw, or as translated by communication devices such as telephones or computers--but not to mere signals that interfere with Internet communication by shutting down computers or clogging bandwidth. [75] That would link section 230 to the tort claims it was designed to regulate; it is fully consistent with the language, history, and policies associated with the Communications Decency Act; and it would free courts to consider the proper contours for ISP liability with respect to issues of cyber-security.

[*255] **B. Common Law Principles**

Not only have courts been expanding the scope of the immunity offered by the Communications Decency Act, they also have been questioning whether common law liability ought to extend to ISPs in the first place. The best discussion we have found of this issue is in *Doe v. GTE Corporation.* [76] The case involved a suit by various athletes who were secretly filmed while undressing in locker rooms. The athletes sued the producers and sellers of the videotapes--Franco Productions and other entities--but, because they correctly anticipated that these defendants would disappear without a trace, the athletes also sued the several ISPs that had hosted Franco's websites. Judge Easterbrook wrote for the panel, and, after resolving some interpretive questions regarding a federal privacy statute and offering some ideas about the

various ways to read section 230 of the Communications Decency Act, he held that plaintiffs had failed to assert a state common law claim. His analysis on this point is why the case is of interest to us.

Easterbrook makes several observations that will be familiar from our discussion. He notes that landlords are not held liable for dangerous activities that occur on their premises; carriers such as Federal Express are not held liable for failing to prevent shipments of dangerous objects; telephone companies are not liable for allowing customers to use phone lines maliciously; and so forth. Easterbrook then suggests that ISPs should be no different:

> That [one of the defendant ISPs] supplied some inputs . . . into Franco's business does not distinguish it from the lessor of Franco's office space or the shipper of the tapes to its customers. Landlord, phone company, delivery service, and web host all *could* learn, at some cost, what Franco was doing with the services and who was potentially injured as a result; but state law does not require those providers to learn, or to act as good Samaritans if they do. The common law rarely requires people to protect strangers, or for that matter acquaintances or employees. [77]

Easterbrook is right that the common law rarely requires anyone to be a Good Samaritan. Where Easterbrook errs, however, is in assuming that ISP liability is best understood as a Good Samaritan rule, rather than as a traditional tort. The distinction is important because, while the common law rarely creates Good Samaritan obligations, it [*256] routinely uses tort law to accomplish similar goals. Thus it is tort law, rather than any Good Samaritan obligation, that pressures drivers to watch out for stranger-pedestrians, and it is again tort law that encourages firms to think twice before polluting a stranger-neighbor's land. Easterbrook never explains why he dismisses ISP liability as if it is some unusual obligation to do nice things for strangers rather than a conventional application of familiar tort law principles. [78]

We are sympathetic if Easterbrook was simply trying to reach the right outcome in the case at hand. It is difficult and perhaps even impossible for ISPs to monitor websites for the sale of illegal videotapes because such tapes cannot easily be distinguished from perfectly legitimate video content. Given those difficulties, we agree that the ISPs sued in this particular case should not have been held accountable for their role in transmitting the tapes. We resist Easterbrook's analysis, however, because in other settings ISPs may be able to do more. Just as a delivery service might be held liable for delivering a package that obviously contains a ticking bomb, or a landlord might be held liable for permitting a use of his premises that is overtly illegal, [79] ISPs might rightly be held liable for permitting malicious behaviors that they could have detected or deterred at reasonable cost. Easterbrook's opinion gives the impression that ISPs ought never be held liable for harms done to third parties. That judgment is over-broad and premature.

## V. CONCLUSION

Controversies over indirect liability have been prominent in recent years, sparked in no small measure by questions over who, if anyone, should be held liable for the rampant copyright infringement that as of this writing continues to be a significant feature of life online. With that in mind, we conclude with some remarks about how our comments on cyber-security relate to that other debate, along the way clarifying the outer limits of our position and also suggesting areas for further research.

At the outset, it must be noted that, on its own terms, indirect liability knows few bounds, and thus there is almost always an argument to bring yet another entity into the chain of liability. In the copyright wars, for example, the first round of litigation was against the websites that facilitate infringement by offering services that directly or indirectly match would-be music uploaders with would-be [*257] music downloaders. [80] The battle soon expanded to ensnare the venture capital firms that fund those entities [81] and even the ISPs that provide the infrastructure over which music piracy takes place. [82] In our setting, one could quite similarly talk about imposing liability on Microsoft, the theory being that the

vulnerabilities in the Windows operating system are akin to the design defects actionable in products liability law, or Dell, for the role its nearly ubiquitous computer systems play in the struggle for cyber-security.

Extending liability in this way would not necessarily be unwise. Microsoft, for example, surely can design its initial software to be less vulnerable to Internet misbehavior. This is simply a matter of investing more resources in product design as well as testing. Microsoft could also redesign its software such that customers would be required to download patches when necessary, perhaps under the threat that the software will stop working if the latest patch is not downloaded within a specified period. This would be a minimally intrusive way to ensure that users keep their antivirus precautions up to date--a bit like mandatory vaccinations for school children. Further, even if Microsoft cannot take additional precautions, we pointed out earlier that the price increase that would result from an increase in liability would itself have some policy allure in that the resulting price would better reflect the relative value of the Windows operating system as compared to competing alternatives like Mac OS.

All that said, however, as a practical matter the chain of liability cannot extend forever, and thus in the end choices must be made as to which entities are best positioned to support enforcement of the law. The right thought experiment is to imagine that all the relevant entities and all the victims and all the bad actors can efficiently contract one to another and then to ask how the parties would in that situation allocate responsibility for detecting and deterring bad acts. Our firm suspicion in the cyber-security arena is that ISPs would in that negotiation end up with significant responsibilities for policing Internet activity; but that might not be true in the copyright setting, and it is certainly a conclusion that might change if there are radical changes in the abilities of other entities to prevent and deter bad acts.

[*258] Another distinction between the literature on copyright infringement and our own inquiry regarding cyber-security comes in understanding the direction of the externality imposed. The possibility of copyright infringement increases the average subscriber's willingness to pay for broadband Internet service. Indeed, music piracy is in many ways the "killer app" that is today driving the deployment of broadband Internet service to the home. As such, there is a silver lining to the bad act of copyright infringement. The opposite is true, however, for worms and viruses, each of which imposes a cost on the average user and thus reduces the incentive to subscribe. This leads to two conflicting implications. One is that policymakers should on this theory be marginally more interested in imposing liability for cyber-insecurity than they are in imposing liability for music piracy; in essence, the former is a barrier to broadband deployment whereas the latter is a camouflaged subsidy. The other implication is that legal rules might at the same time be less necessary, because ISPs already have a strong incentive to improve cyber-security (subscribers favor it) whereas ISPs have no similar incentive when it comes to fighting copyright infringement.

Yet another important distinction is that the copyright dispute is in many ways a dispute about the propriety of the underlying property right, not a dispute about the proper contours of indirect liability per se. Many of those who oppose liability in the copyright setting also question, in a more fundamental way, the scope and duration of federal copyright grants. That radically alters the nature of the debate as compared to our setting, where there is widespread agreement that worms, viruses, and denial-of-service attacks are rightly deemed illegal and the real question comes only in determining how best to discourage these counterproductive behaviors.

Finally, the copyright dispute is one where there are a variety of plausible legal responses, and thus policymakers must tread carefully as they try to determine which approach offers the best balance in terms of costs and effectiveness. Is the best approach to facilitate lawsuits against the specific individuals who upload and download music? [83] Would it be better to recognize indirect liability as a supplement to direct liability or even a substitute for it? [84] What about the idea of rejecting legal responses entirely and encouraging instead self-help [*259] techniques like more effective encryption of digital content? [85] These are plausible questions in the copyright setting; parallel questions in the context of cyber-security, however, ring hollow. That is, as we have already emphasized, holding individuals directly responsible for worms and viruses is all but impossible given that individual bad actors are so difficult to track and,

even when identified, usually lack the resources necessary to pay for the damage they cause. And, as we have also pointed out, while self-help techniques like firewalls and antivirus software do have a role to play in improving cyber-security, it is hard to imagine that these sorts of precautions can be a sufficient response to the problem, let alone a response that is so attractive as to justify blanket immunity for ISPs. The viability of alternative legal strategies is thus a final important distinction to draw between these two settings. The existence of such strategies should give pause to advocates and critics alike in the copyright debates, but they seem significantly less salient when it comes to the question of whether ISPs should be liable for their role in creating and propagating malicious Internet code.

**Legal Topics:**

For related research and practice materials, see the following legal topics:
Computer & Internet LawCopyright ProtectionCivil Infringement ActionsDefensesInnocent IntentComputer & Internet LawInternet BusinessInternet & Online ServicesService ProvidersComputer & Internet LawInternet BusinessInternet & Online ServicesTypes

**FOOTNOTES:**

n1 See, for example, the Electronic Communications Privacy Act, Pub L No 99-508, 100 Stat 1848 (1986), codified as amended in scattered sections of 18 USC; and the Computer Fraud and Abuse Act, Pub L No 98-473, 98 Stat 1837, 2190 (Oct 12, 1984), codified as amended at 18 USC ? 1030 (2002).

n2 Bob Keefe, *Microsoft Beefs up Security Initiatives,* Atlanta J-Const 3C (Feb 25, 2004).

n3 See, for example, Brian McManus, *Rethinking Defamation Liability for Internet Service Providers,* 35 Suffolk U L Rev 647 (2001) (advocating a return to common law standards for liability in the context of defamation law); Assaf Hamdani, *Who's Liable for Cyberwrongs?,* 87 Cornell L Rev 901 (2002) (articulating an intricate liability regime for a variety of online wrongs).

n4 47 USC ? 230 (c)(1).

n5 17 USC ? 512(a).

n6 17 USC ? 512(c)-(d).

n7 We discuss and criticize several of these cases in Part IV.

n8 The Communications Decency Act is an immunity provision in that it eliminates liability for a certain class of actions without explicitly making that immunity contingent on particular precautions. The Digital Millennium Copyright Act, by contrast, is a safe harbor provision, in that it creates immunity but only for entities that take specific precautionary steps. Interestingly, some commentators have suggested that the Communications Decency Act should be read as a safe harbor provision, with its immunity applying only where the relevant service provider has itself attempted to block indecent or otherwise inappropriate communications. See Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content,* 88 Va L Re 206, 217 n.61 (2002). No court has yet adopted that view, although it is attractive on policy grounds and seems consistent with both the language of the act and its structure. See *Doe v GTE Corp,* 347 F3d 655, 660 (7th Cir 2003) (discussing interpretations of section 230 immunity that would nevertheless encourage filtering by ISPs).

n9 47 USC ? 230 (c)(2)(A).

n10 17 USC ? 512 (g)(1).

n11 See, for example, *Herbert v Shanley Co,* 242 US 591 (1917) (holding that a hotel owner can be

held liable when copyrighted work is performed at the hotel without permission).

n12 See Restatement (Second) of Agency ? 216.

n13 Neal Kumar Katyal, *Criminal Law in Cyberspace,* 149 U Pa L Rev 1003, 1007-08 (2001). Katyal does not in the end oppose liability for Internet service providers. As he writes later in the article, his point "is not to suggest that third-party deterrence is always inappropriate, but simply to caution that there are tough calculations to work out." Id at 1098.

n14 Hamdani, 87 Cornell L Rev at 918 (cited in note 3). Other scholars, and indeed some courts, have raised similar concerns. See, for example, Neil Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing,* 17 Harv J L & Tech 1, 13 n30 (2003) ("ISPs do not fully share the benefits its subscribers derive from placing material, whether infringing or non-infringing, on the network. As a result, imposing liability on ISPs for subscribers' infringing material induces ISPs to overdeter, purging any material that a copyright holder claims is infringing."); *Zeran v America Online,* 129 F3d 327, 333 (4th Cir 1997) ("Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon [accusation], whether the contents were defamatory or not.").

n15 We are not just splitting hairs. For example, because of the way he phrases the problem, Hamdani wrongly concludes that there is no problem with overzealous enforcement in cases where the subscriber uses in-house equipment rather than purchasing access in the competitive market. In such a case, subscriber benefits are fully internalized by the ISP (which satisfies Hamdani) and yet the mismatch between private and social benefits remains. See Hamdani, 87 Cornell L Rev at 918-20 (cited in note 3). More generally, by framing the problem as they do, Katyal and Hamdani leave their arguments open to a simple response: ISPs should raise prices and in that way capture a larger share of subscriber utility. This is surely not what Katyal and Hamdani have in mind, and the reason is that they, like us, are actually worried about the problem of positive externalities.

n16 47 USC ? 230 (b) (3).

n17 47 USC ? 230 (b) (4).

n18 The terminology used for this concept varies considerably in the literature. Economists seem to prefer the phrase "vicarious liability" even though, in copyright law at least, vicarious liability is merely one specific type of indirect liability, namely liability that attaches because the third party has control over the direct bad actor and also benefits from the bad acts in question. See Douglas Lichtman and William Landes, *Indirect Liability in Copyright: An Economic Perspective,* 16 Harv J L & Tech 395, 396-99 (2003). Other commentators use phrases like "secondary liability" or "third-party liability" to capture the intuition that this is liability that attaches not to the bad actor directly, but to some other related party. In any event, we use the term "indirect liability" as our generic phrase.

n19 See Restatement (Second) of Agency ? 216.

n20 North Dakota's dram shop statute, for example, provides that any person "injured by any obviously intoxicated person has a claim for relief . . . against any person who knowingly disposes, sells, barters, or gives away alcoholic beverages to a person under twenty-one years of age, an incompetent, or an obviously intoxicated person." D Cent Code 5-01-06.1 (2003). Arizona law, by contrast, immunizes from liability parties who merely furnish or serve "spirituous liquor to a person of the legal drinking age." Ariz Rev Stat Ann 4-301, 4-311 to -312 (West 1995).

n21 This is usually done as a matter of statute. See Dan B. Dobbs, *The Law of Torts* 934 (West, 2000).

n22 See, for example, *Sharp v W.H. Moore, Inc,* 796 P2d 506 (Idaho 1990).

n23 See, for example, *Fonovisa v Cherry Auction,* 76 F3d 259 (9th Cir 1996).

n24 See Restatement (Third) of Products Liability, ? 402A. We could go on with a variety of other examples. Perhaps most eerily similar to our current topic: a physician can be held liable for failing to warn a patient's spouse that the patient is carrying, and thus might expose the spouse to, a real-world ailment like Rocky Mountain Spotted Fever. See *Bradshaw v Daniel,* 854 SW2d 865 (Tenn 1993) (holding that a physician had, and failed to fulfill, a duty to warn patient's wife of one such health risk).

n25 For a general introduction, see Alan Sykes, *Vicarious Liability,* in Peter Newman, ed, 3 *The New Palgrave Dictionary of Economics and the Law* 673 (Palgrave Macmillan, 1998).

n26 Among these constraints are (1) the costs a victim would incur to identify and then sue the liable parties, and (2) cognitive limitations that might lead to incorrect predictions regarding the likelihood or extent of any expected accidents.

n27 We assume that the indirectly liable parties are subject to the effective reach of the law, which is to say that they can be identified and they have sufficient assets to pay for any harms they might cause. While that is typically true, it is not always true, especially in instances where the harm in question is catastrophic.

n28 Our discussion follows the analysis in Steven Shavell, *Economic Analysis of Accident Law* 170-75 (Harvard, 1987); Alan Sykes, *An Efficiency Analysis Of Vicarious Liability Under the Law of Agency,* 91 Yale L J 168 (1981); Alan Sykes, *The Economics of Vicarious Liability,* 93 Yale L J 1231 (1984); Alan Sykes, *The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines,* 101 Harv L Rev 563 (1988); Reinier Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy,* 2 J L & Econ 53 (1986). Two helpful overviews are Sykes, *Vicarious Liability* (cited in note 25), and Reinier Kraakman, *Third Party Liability,* in Peter Newman, ed, 3 *The New Palgrave Dictionary of Economics and the Law* 673 (Palgrave Macmillan, 1998).

n29 See, for example, *Sharp v W.H. Moore, Inc,* 796 P2d 506 (Idaho 1990); *Fonovisa v Cherry Auction,* 76 F3d 259 (9th Cir 1996).

n30 The right question to ask is whether the employer can influence the relevant employee behavior more effectively than can the state. Thus, while an employer can fine an employee for bad acts committed on the employee's own time, and while such a system could be used to discourage bar fights and spousal abuse, the government can implement such a system of fines just as easily, and the government might even be better suited to do so because, for example, the government has the ability to incarcerate bad actors for whom the fine turns out to be an insufficient disincentive.

n31 See Sykes, *Vicarious Liability* (cited in note 25) (discussing employee torts outside the scope of employment). Note that there might be more of a link here than we indicate above. An employer who places enormous stress on his employee, for example, surely increases the likelihood that that employee will abuse his spouse or become involved in barroom brawls. Thus there might be at least a small activity-level effect to consider, and certain types of employers should perhaps bear liability for employee behavior that takes place after hours.

n32 For a discussion, see *Goldberg v Lee Express Cab Corp,* 634 NYS2d 337 (1995).

n33 This is similarly a good reason for courts to look askance at Grokster, the entity that intentionally designed its peer-to-peer music trading system such that, once activated, the technology (arguably) cannot effectively monitor for copyright infringement. On the general theme of intentional ignorance in the context of indirect liability, see *In re Aimster Copyright Litigation,* 334 F3d 643, 650-51 (7th Cir 2003) (arguing that "a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which

the service is being used").

n34 Erich Luening and Wylie Wong, Virus set for Jan 1, 2000, CNET News.com, online at http://news.com.com/Virus+set+for+Jan.+1,+2000/2100-1001_3-233907.html (Dec. 3, 1999).

n35 See Alison Langley, *Computer Viruses Are Frustrating Insurers, Too,* NY Times S3 P4 (Oct 12, 2003). Insurers refuse to provide substantial insurance against many kinds of malicious attacks, especially viruses and worms, because the risks are not independent.

n36 There are second-order concerns as well, such as the fact that defendants will invest more resources resisting long sentences than they will short ones. There are also equitable concerns, as it might seem inappropriate to establish a legal system where, by design, only a small fraction of the culpable parties are punished, but those that are punished suffer extraordinarily large penalties. Lastly, it is often important to keep penalties low enough that there is a plausible threat of an additional penalty if the relevant bad actor further misbehaves. Otherwise, after crossing the relevant threshold, bad actors have no incentive to mitigate the harm they cause.

n37 For an introduction to these interconnection issues, see Stuart Benjamin, Douglas Lichtman and Howard Shelanski, *Telecommunications Law and Policy* 915-25 (Carolina Acad Press, 2001).

n38 Bounded rationality might be an additional limitation on the ability of Internet subscribers to efficiently create the optimal indirect liability regime through private contracts. The many users who today are still clicking to execute email attachments from strangers are as a practical matter unlikely to be sufficiently rational contract negotiators. Their blind spots undermine any argument that private parties will, if left to their own devices, be able to efficiently shift and allocate responsibility for online security.

n39 An automatic update system like the one we propose would become an attractive target for hackers because it could conceivably be used to corrupt a large number of computers simultaneously. Then again, the current voluntary system suffers the same flaw, albeit on a slightly smaller scale.

n40 The right approach might be to empower government officials to require ISPs to store information without any particular showing or court order, but then to permit government officials to access that information only with a court order in hand. This would free the government to act quickly in terms of preserving evidence, but it would still respect privacy interests until the government could make a sufficient case. This approach has many virtues: for instance, it preserves evidence during that gap between when the government first becomes suspicious and when the government can corroborate its suspicions, a gap during which evidence today is often lost; and it allows for narrow searches of the stored information to be followed up with broader searches in cases where later events suggest that there is more to be learned from the stored data. Computer scientist Carl Gunther has been working on various technologies along these lines, and he was helpful in explaining these technologies to us.

n41 See discussion in Part II.

n42 The disincentive discussed above perfectly calibrates activity levels in situations where externalities are sufficiently symmetric. Imagine a simple such case: a world with three subscribers where each imposes on each of the other two a negative externality of two dollars. The first subscriber in this setting imposes four dollars worth of harm, namely two dollars imposed on each of two peers, but also suffers a total of four dollars worth of harm, again two dollars from each of two peers. To the extent that similar sorts of symmetry might be created in the ISP setting--for example, by forcing each ISP to serve a similar population--activity levels could be calibrated without the introduction of legal liability.

n43 The details turn out to be slightly more complicated, as DSL prices are distorted by the unbundling rules of the Telecommunications Act of 1996, which in essence require existing local telephone companies to rent their infrastructure--including DSL capability--to rivals at regulated rates. For an introduction to the issues, see Benjamin, Lichtman and Shelanski, *Telecommunications Law* at 715-755

(cited in note 37).

n44 If the social costs exceed the social benefits, by contrast, there is no problem, because under this condition the subscriber should not be online.

n45 One way to think about this economic problem is to note that connecting to the Internet is a prerequisite to shopping online, talking with friends, receiving advertisements, and so on; and that this is an expensive prerequisite both in terms of the price charged, and in terms of the frustration experienced by users who are not quite computer literate. Knowing this, parties that benefit from having the marginal subscriber online will attempt to compensate that subscriber by, for example, offering sale prices. But there are two limitations on that approach. One is that some parties have no clear mechanism by which to reward the marginal consumer. The other is that there will be some free-riding, which is to say that some parties with the ability to reward the marginal consumer will choose not to, hoping that other parties will sacrifice sufficiently to induce the subscription. This latter problem is actually a generic problem that plagues any market where there is some form of a prerequisite, as Lichtman explains more fully in Douglas Lichtman, *Property Rights in Emerging Platform Technologies,* 29 J Legal Stud 615 (2000).

n46 Internet Tax Freedom Act, Pub L No 105-277, 112 Stat 2681, 2719 (1998) (included as Title XI of the Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1999).

n47 These subsidies were originally put in place when the Internet was in its infancy and the market for Internet service was therefore subject to rapid and unpredictable change. Now that the market has matured, any justification along those lines seems less valid, but the issues identified in the text suggest that the subsidies perhaps should remain.

n48 Again, for more information, consult Benjamin, Lichtman and Shelanski, *Telecommunications Law* at 614-623, 712-714, 768-791 (cited in note 37).

n49 Telephone companies do this, exchanging cash when one company originates a call that another company terminates. See id at 749-55, 927-45.

n50 Then again, changing the identity of the buyers might have beneficial effect, as ISPs are surely more educated consumers. The only obvious concerns would be: (1) if ISPs enjoy sufficient market power that they would be able to arrogate to themselves more of the benefits created by innovative third-party security options, thereby depressing other firms' incentives to create those new options in the first place; and (2) the worry that regulations applicable to ISPs might somehow interfere with their ability to purchase security assistance through normal market interactions.

n51 See Shavell, *Economic Analysis* at 277-85 (cited in note 28).

n52 For a discussion of these concerns in other contexts, see Jennifer Arlen, *The Potentially Perverse Effects of Corporate Criminal Liability,* 23 J Legal Stud 833 (1994); C. Y. Cyrus Chu and Yingyi Qian, *Vicarious Liability Under a Negligence Rule,* 15 Intl Rev L & Econ 205 (1995).

n53 See supra note 29 and accompanying text.

n54 See, for example, *High School Student Admits Creating 'Sasser' Internet Worm,* Chi Trib A11 (May 10, 2004) (reporting that the creator of a worm was arrested in Germany).

n55 In theory, a state involved in some cooperative enterprise with other states can always sanction a free-rider by bombing, cutting off trade, and so on, but in practice states almost never do this within particular treaty regimes. For example, when France failed to allow a certain kind of Pan Am jet to land in Paris--an apparent violation of the Civil Aviation Convention--the United States retaliated not by banning trade in some important commodity, but instead by forbidding Air France to land flights in Los Angeles. See *Case Concer the Air Serv Agr Between France and the United States,* 18 UNRIAA 417 (1978). It is

an interesting question as to why states usually retaliate "in kind" rather than via substitutes, but, whatever the reasons, the pattern seems relatively robust.

n56 This history is recounted in virtually all of the cases involving ISP liability for defamation, and it is also echoed in nearly all of the scholarly commentary that was written in response. See, for example, *Cubby, Inc v Compuserve, Inc,* 776 F Supp 135, 139-40 (SD NY 1991); Ray Ku, *Irreconcilable Differences?: Congressional Treatment of Internet Service Providers as Speakers,* 3 Vand J Ent L & Prac 70, 73-77 (2001). Interestingly, most of these sources neglect to mention that there exists a third common law category consisting of telephone companies, mail carriers, and similar conduits, and that these entities typically enjoy complete immunity because they lack the authority to filter or otherwise discriminate based on content. On conduits, see *Lunney v Prodigy Servs,* 94 NY2d 242, 249 (1999).

n57 *Cubby, Inc v Compuserve, Inc,* 776 F Supp. 135, 139-40 (SD NY 1991).

n58 Id at 140.

n59 *Stratton Oakmont v Prodigy Services,* 23 Media L Rep (BNA) 1794 (NY Sup Ct 1995).

n60 Id at 10 (internal citations omitted).

n61 This echoes the concerns we expressed earlier regarding strategic ignorance. See note 33 and accompanying text.

n62 47 USC ? 230(c)(1).

n63 *Zeran v America Online,* 129 F3d 327 (4th Cir 1997).

n64 Id at 330.

n65 Id at 332.

n66 Id.

n67 Id at 333-34. The court also worried that "notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services" because "efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability." Id at 333. That strikes us as a fear that can be easily addressed, specifically by applying some form of a "knew or should have known" standard. That is, an ISP should not be allowed to shield itself from liability simply by choosing not to investigate. Whether an ISP investigates or not, if it should have known about a particular statement, it should be held accountable. Again, this is the concern about parties hiding their heads in the sand, first mentioned in note 33 and accompanying text. Standards that use the "knew or should have known" structure avoid this problem--under such a standard, there is no incentive to remain ignorant--whereas standards that turn on actual knowledge do not.

n68 See, for example, David Sheridan, *Zeran v AOL and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet,* 61 Alb L Rev 147 (1997); Lyrissa Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace,* 49 Duke L J 855 (2000).

n69 See *Barrett v Rosenthal,* 12 Cal Rptr 3d 48 (Cal 2004) (pending appeal from lower court findings with respect to statutory construction and legislative history of section 230); *Grace v eBay, Inc,* 2004 WL 2376664 (Cal 2004) (similar appeal also pending).

n70 See 17 USC ? 512(c)(3)(A) (requiring that a complainant submit, among other things, a statement under penalty of perjury certifying that the complainant is providing accurate information regarding the

alleged infringement and that the complainant is either the owner of the copyright in question or an authorized agent representing that owner).

n71 *Green v America Online,* 318 F3d 465 (3d Cir 2003).

n72 Id at 469. John Doe 1 and another user also allegedly posted defamatory statements about Green.

n73 Id.

n74 Id at 471.

n75 Consistent with our remarks at the start of this section, we would be equally happy to see Congress amend the Communications Decency Act in this manner.

n76 *Doe v GTE Corporation,* 347 F 3d 655 (7th Cir 2003).

n77 Id at 661 (emphasis in original).

n78 For some insight into where to draw the line, see *Stockberger v United States,* 332 F 3d 479, 481 (7th Cir 2003) (Posner, J.) (suggesting reasons not to compel rescues and other magnanimous behaviors).

n79 See, for example, *Fonovisa v Cherry Auction,* 76 F.3d 259 (9th Cir 1996).

n80 See *A&M Records, Inc v Napster, Inc,* 239 F 3d 1004 (9th Cir 2001); *In re Aimster Copyright Litigation,* 334 F 3d 643, 650-51 (7th Cir 2003); *MGM Studios, Inc v Grokster, Ltd,* 259 F Supp 2d 1029 (CD Cal 2003).

n81 The venture capital firm of Hummer Winblad, for example, was sued for its role in funding Napster. See Mark A. Lemley and R. Anthony Reese, *Reducing Digital Copyright Infringement Without Reducing Innovation,* 56 Stan L Rev 1345, 1346 (2004).

n82 See *RIAA v Verizon Internet Servs,* 351 F 3d 1229 (DC Cir 2003) (dispute over the conditions under which an ISP must identify subscribers who are accused of being involved in online infringement).

n83 Some commentators believe so and argue that copyright law should reject indirect liability and instead focus on procedural reforms that would make direct lawsuits less costly. See, for example, Lemley and Reese, 56 Stan L Rev 1345 (cited in note 81). The challenge for these commentators comes in squaring their argument with the real world empirical data: thousands of lawsuits have been filed, and yet illegal file swapping continues, largely undeterred.

n84 For discussion, see Lichtman and Landes, 16 Harv J L & Tech 395 (cited in note 18).

n85 For one effort along these lines, see Implementation of Section 304 of the Telecommunications Act of 1996, 18 FCC Rcd 20885 (2003) (requiring hardware manufacturers to cooperate with efforts to encrypt digital content distributed via cable and broadcast television). Interestingly, the possibility of self-help has posed a significant challenge to the federal government's efforts to control the online distribution of offensive material that is inappropriate for minors. The problem? The Supreme Court seems to think that filters installed by home users can be so effective that they render more heavy-handed restrictions on speech--like the Child Online Protection Act--unconstitutional. See *Ashcroft v ACLU,* 124 S Ct 2783 (2004).