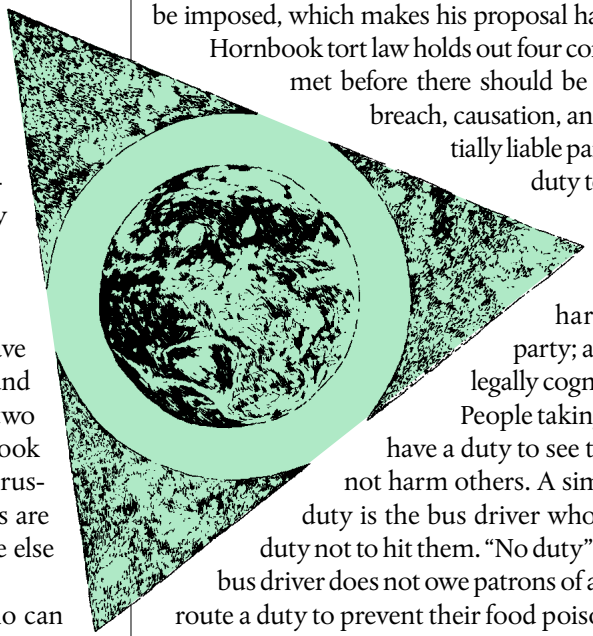
Do ISPs have a duty to protect the world?

Against ISP Liability

By Jim Harper
Cato Institute

A signal benefit of tort rules developed at common law is how efficiently they apportion responsibility for protections from harm. But efficiency alone does not qualify a proposed rule to be law. In "Holding Internet Service Providers Accountable" (Winter 2004), Douglas Lichtman argues for making Internet Service Providers (ISPs) liable for the propagation of Internet pathologies like worms, viruses, and other malicious computer code. His hope is that placing liability on ISPs will give them the incentive to protect Internet users.

Protecting Internet users is a noble goal and Lichtman has given this problem a good deal of thought. But his argument for ISP liability has a fundamental flaw: it places efficiency ahead of justice. The Internet is a medium, not a thing, and the supply of access to it is peculiarly unsuited to a liability rule like Lichtman proposes.



LICHTMAN'S CASE

When wrongdoers are identifiable and when they have sufficient assets, they can be brought into court and required to make victims whole. But when those two conditions do not apply, Lichtman tells us, we can look for other parties to hold liable. The authors of the viruses that swarm the Internet and damage computers are hard to find and have few assets. Perhaps someone else should be responsible for their behavior.

A suitable target for indirect liability is one who can detect and deter another's bad acts and who would be encouraged by a liability rule to "internalize some significant negative externality unavoidably associated with its activities." ISPs are a natural choice, says Lichtman, because of their ability to screen users' communications. Even if ISPs cannot control every harmful use of the Internet, a second rationale for liability holds that the increased price of Internet service (because of ISPs' preventive measures and payouts) could ratchet back the careless, and therefore dangerous, use of the Internet by the inexperienced.

Holding ISPs liable sounds like a way to reduce Internet wrongs. But is it right?

ON DUTY

Lichtman is not clear about what form of indirect liability should be imposed, which makes his proposal hard to counter-argue.

Hornbook tort law holds out four conditions that must be met before there should be direct liability: duty, breach, causation, and damages. A potentially liable party must have owed a duty to the injured party; it must have breached that duty; that breach must have harmed the injured party; and the harm must be legally cognizable as damages.

People taking actions of any kind have a duty to see that those actions do not harm others. A simple case illustrating duty is the bus driver who owes pedestrians a duty not to hit them. "No duty" is just as simple: The bus driver does not owe patrons of a restaurant along his route a duty to prevent their food poisoning.

The duty requirement ultimately rests on bare policy assertions about who should look out for whom, but it has some clear outer limits. Tort law does not obligate strangers to protect each other from harm; rather, it compensates the injured from the purses of wrongdoers.

Embedded in the duty requirement is a theory of justice: People should be accountable for their own actions. People

Jim Harper is director of information policy studies at the Cato Institute. He may be contacted by e-mail at jharper@cato.org.

should not be made accountable for the actions of others. We should not deviate lightly from this sort of justice.

Indirect liability is an unusual exception to the duty requirement—perhaps not unusual enough. Dram shop laws, the doctrine of negligent entrustment, some copyright enforcement law, some landlord-tenant laws, and the foreseeable misuse doctrine in product liability law all have greater or lesser strains of indirect liability. Such laws push parties into monitoring and controlling the behavior of others—even, sometimes, if those others are free, responsible actors subject to effective reach of the law.

Lichtman uses employer liability as his template for ISP liability because it is the easiest case. Employees acting in the scope of their employment are working for the direct benefit of the employing enterprise. The maxim of *respondeat superior,* holding that an employer may be liable to those harmed by an employee, is a comfortable one to bear.

But creating liability based on connecting computers to the Internet is not similarly comfortable. No (surviving) theory of justice supports assigning ISPs a duty to protect the world's Internet users merely because they transfer bits from one place to another for their clients.

Lichtman speaks of ISPs as having "immunity" from liability for Internet pathologies, but that assumes the case he is trying to make: ISPs should be liable in the first place. An immunity is an exception to liability that would otherwise pertain, granted on the grounds that some greater good comes from immunizing the actor. The Communications Decency Act and the Digital Millennium Copyright Act are both styled as immunities because they were enacted to smooth roiling waters about the scope of ISP liability for their clients' content and communications. Congress's enactment of those two laws does not show that ISPs were otherwise appropriate targets of liability.

Had common law processes been left to determine ISPs' liability, a variety of courts would have weighed the competing interests through strings of real-world decisions over several years. As likely as not, they would have concluded that ISPs have no duty to protect the world from their clients. What Lichtman calls the "recent push to immunize" ISPs may be no more than growing recognition that they do not owe the world a duty.

Hosting, of course, is where we have the most experience with questions about ISP liability. Hosting is the close case because content sits at a fixed address on an ISP's servers, often in one of a few formats suitable for the World Wide Web. Lichtman's argument appears to call for making ISPs liable in their capacity as providers not of hosting, but of Internet access. As shown by the structure of the Digital Millennium Copyright Act, and by the *RIAA v. Verizon* case litigating it, there is a substantial difference between hosting Internet content and providing Internet access. Internet access service is the transfer of bits—any bits—to or from clients' systems.

ON PRIVACY

Should ISPs be reading those bits? Lichtman has seriously underweighted privacy in his argument for ISP liability. Part of what users bargain for when they engage an ISP is privacy: the assurance that the data they transmit will not be monitored, copied, held in storage, or shared beyond what is necessary to provide good service and comply with law. ISP business models that traded on user information—offering lower prices in exchange for the right to sift through user data—have gone by the wayside.

People should not be made accountable for the actions of others. We should not deviate lightly from this sort of justice.

As an aside, Lichtman says he would reject liability for telephone companies that fail to suppress crank calls, citing "obvious" privacy concerns. The quantum, detail, and breadth of information ISPs carry are head and shoulders—if not orders of magnitude—above what telephone companies carry. And ISPs transmit material in digital form, which is relatively easy to collect, copy, and interpret (unless it is encrypted). The stakes for privacy in the ISP context are quite a bit higher, not lower, than in the provision of telephone service. As access providers, ISPs should no more copy or interpret the bits they transfer than phone companies should listen in on calls or the U.S. Postal Service should read the mail it delivers.

Lichtman suggests that liable ISPs would monitor their users for unusual behavior or perhaps store users' data streams for a period of time. Versions of those ideas are hot debates already. Under the Communications Assistance to Law Enforcement Act, U.S. law enforcement authorities are seeking to require providers of Voice over Internet Protocol service to build wiretapping capabilities into their systems. European law enforcement authorities seem never to give up on proposals to require ISPs to retain client data streams for their investigative purposes. A liability regime that would promote those practices is not a step to take blithely.

SUPPRESSING MARKET RESPONSES

Some ISPs do review clients' data as they provide contagion-control services, including anti-spam, anti-spyware, and antivirus

MORGAN BALLARD

protections. Internet users also hire separate service providers to protect against those pathogens. Some such offerings filter content while it is on the network; others do so after it arrives at the computer. What they do with harmful or suspect content varies with the needs, tastes, and sophistication of users. There is a well-developing and diverse market for Internet hygiene services that Lichtman's proposal would suppress.

A second layer of market response is revealed by complaints about the susceptibility of popular software to Internet pathogens. Microsoft's Windows operating system and Internet Explorer browser are subject to competition along the security axis (and all others) from Mac OS X and Firefox, for example. Microsoft will undoubtedly lose market share as long as it is perceived as failing to match or exceed the security qualities of the competition. (Lichtman nowhere argues for software makers' liability—direct or indirect—though his arguments for indirect liability apply equally well to them.)

Yet another set of service providers, mostly serving large institutions, probe systems for known and emerging vulnerabilities. When they discover a weakness, it is reported so that the latest fixes can be applied. Those services mostly protect against hacking, but they assuredly also provide protection against some of the threats Lichtman wishes to reach.

Users are, and must remain, responsible for themselves, of course. Several forms of Internet contagion use "social engineering"—that is, they manipulate human interests and gullibility—to do their work. The Kournikova worm spread as far as it did by posing as a picture of the popular Russian tennis pin-up. Common phishing scams rely on less exotic but no less dangerous copying of the look and feel of popular financial services Web sites.

On the margin, pushing disproportionate liability onto ISPs would erode Internet users' focus on self-awareness and self-help, just as it would erode the market for expert service providers and for more-secure software. Lichtman admits the validity of that objection but argues that the logical implication of market responses "is not complete immunity for ISPs." Calling it "immunity," again, assumes what Lichtman has not shown: that ISPs should be liable.

Lichtman concedes that ISP liability should be "tailored" in light of the possibility that it would create moral hazard elsewhere. Perhaps this retreat should stop at the line where ISPs have a duty to protect—that is, at traditional principles for liability.

OVERZEALOUS PROVIDERS

The other major objection Lichtman addresses is the problem of the overzealous provider. Holding ISPs liable for customers' online behavior would lead them to charge more and suppress beneficial content and activity—often zealously, sometimes overzealously. Lichtman assumes too easily that the network effect would keep Internet subscription levels high even when ISPs were overzealous in protecting themselves from indirect liability.

The "network effect" is the idea that the value of a networked good or service is roughly proportional to the square of the number of customers already owning that good or using that service. Lichtman says that he and Amazon.com benefit enough from the Internet presence of relatively unsophisticated parties like his mother that they would cajole her and contribute to her ISP fees, if necessary, were those fees pushed higher by ISP liability.

One reason why the Internet's network effect is so strong, though, is the ability people have to communicate and transfer data free of inhibition. Liability for Internet pathologies would lead ISPs to monitor, collect, and suppress outbound e-mail, peer-to-peer file transfers, use of File Transfer Protocol, instant messaging, and even comments submitted to blogs, all of which are potential routes for transferring harmful code. The policy Lichtman argues for would reduce the network effect.

Consider the Internet access market and the viability of the network effect if ISPs were liable for copyright violation, obscenity, and defamatory statements put out by their clients. Looking at potentially massive payouts, ISPs would screen content thoroughly, charging clients substantially higher sums for the service. They would restrict their clientele to established media companies and sophisticated, wealthy parties who could indemnify them.

Under such a regime, the Internet might be about where digital cable systems are, with lots of downstream content and very little opportunity for interactivity, much less individual publishing. The robust, democratized, one-to-all medium we have today—attractive enough to make a user out of ordinary folks like Lichtman's mother—was not a foregone conclusion in its early years. The "overzealous" provider might in reality be a quite prudent provider. Posting a bond to chat with Mom would defeat network effects.

A MEDIUM DOESN'T FIT

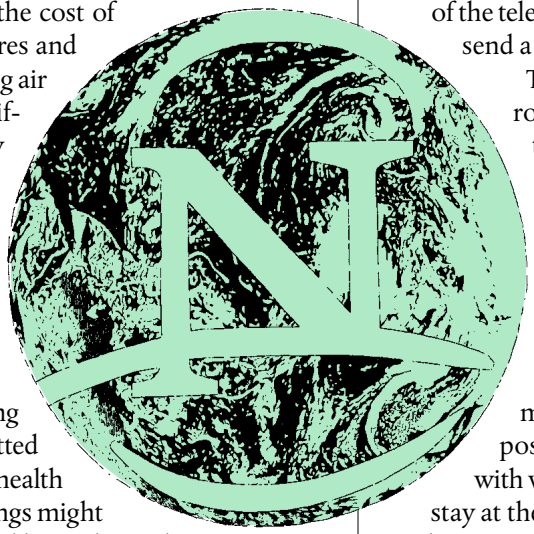
The Internet is the product of wide agreement to use a language called Transmission Control Protocol/Internet Protocol. Using this language, computers can move any data people want, breaking down text, sounds, images, or video to be reassembled by the computer at the other end. In essence, the Internet is a medium. Lichtman's argument joins a very interesting question: Should providing access to a medium obligate the provider to control its use?

We might consider familiar media like paper or radio waves to come up with analogies. But the strongest is another, even more familiar, medium that transfers sounds like the Internet,

and allows light to pass unhindered (over limited distances). It also transfers molecules. That medium is air.

An essential part of what airlines, commercial buildings, and hotels provide their clients is a carefully conditioned air supply. Through the air, their clients do lots of wonderful things, but they also distribute unpleasant odors and offensive sounds. Most relevant here, air also propagates a wide variety of viruses and germs. Those pathogens sometimes kill and often sap productivity, causing billions of dollars in damage annually.

Commercially provided air transmits contagion from parties beyond effective reach of the law because the disease carriers cannot be readily identified. Commercial air providers are well positioned to better sanitize air. If retrofitting existing buildings with stronger air systems is necessary, the imposition will drive up the cost of entering commercial enclosures and move people outdoors, causing air providers to internalize a significant negative externality unavoidably associated with their activities.



This is not *reductio ad absurdum*, but rather the application of Lichtman's framework to the medium of air in modern enclosed spaces. A regime of indirect liability for supplying air in which disease is transmitted could improve overall societal health efficiently. But a lot of odd things might be done if efficiency, unfettered by traditional notions of justice, were to take hold of the tort law.

In the provision of air supply, even direct liability has not taken hold. There were a few transmissions of Severe Acute Respiratory Syndrome in airplanes during the global outbreak in 2003. The episode reveals that airlines could one day owe a duty to their passengers to provide unusual health precautions, but this is not the case today.

As our understanding of disease transmission progresses and as risk tolerances evolve, direct liability for transmitting disease may result. There have been criminal prosecutions for knowing transmission of the AIDS virus. But, in the meantime, disease prevention (airborne and otherwise) is assigned largely to its victims through social expectations that they wash their hands, drink plenty of liquids, avoid risky behavior, eat sensibly, dress warmly, and see the doctor when unusual symptoms arise.

Similar admonitions apply to Internet users: They should install and update antivirus software, patch general purpose software, use a firewall, avoid risky behavior, and install and update anti-spyware software. The list of sensible self-protections will undoubtedly grow.

Media like air or the Internet are incredibly versatile and useful. They transmit a dazzling variety of communications and objects (be those objects molecular or digital). The versatility of those media makes them uniquely unsuited to useful capture by rules such as the one Lichtman has proposed.

CONCLUSION

George Gilder wrote in 1993 about the superiority of dumb networks to smart ones. The traditional telephone system is a smart network, with millions of specialized switches and computers that route and forward signals, establish circuits, collect billing information, and, ultimately, transmit sound along a wire, encoded in electromagnetic waves. The "smarts" of the telephone system allow people to talk remotely, or send a fax, slowly.

The Internet is dumb. It only does one thing: route packets of information wherever they say they should go. This dumb, ingenious network allows far cheaper, faster transmission of text, images, data, sound, video, and two-way voice. What makes the network ingenious is that all the smarts and power lie at the edges.

Internet policy must follow the design of the Internet itself. Just as the computing power lies at the edges of the Internet, so too must the responsibility. To the maximum extent possible, responsibility for wrongdoing must stay with wrongdoers. Responsibility for protection must stay at the edges with users.

There are no panaceas, of course. Keeping responsibility at the edge of the network requires getting better at hunting down bad people. It requires Internet users and their service providers to be more aggressive about self-protection. Both of those things are happening.

In a small but important way, Lichtman's proposal would drive responsibility from the edge of the network toward the center. By forcing intelligence into the middle of the network, ISP liability would push the Internet from a wide-open network toward something far more sclerotic.

His idea is not the only proposal that would have this result. European and third-world regulators in the International Telecommunications Union are formulating plans to capture control of "Internet governance." They would undoubtedly use such control to pursue "public interest" values that conflict with the myriad private interests served so well by an unfettered Internet. That idea and the idea of indirect liability for ISPs are advanced by well-meaning, thoughtful people who are concerned with solving serious problems. Alas, they would capture the Internet rather than the genius of the Internet. R