No. 12-19
June 2012

WORKING PAPER

INTERNET SECURITY WITHOUT LAW: How Service Providers Create Order Online

By Eli Dourado

MERCATUS CENTER
George Mason University

Internet Security without Law: How Service Providers Create Order Online

Eli Dourado
edourado@gmu.edu
Eli Dourado is a research fellow at the Mercatus Center at George Mason University with the Technology Policy Program. His research focuses on Internet governance, the economics of technology, and political economy. Prior to joining Mercatus, Eli worked at the Bureau of Economic Analysis and the U.S. House of Representatives. He holds a BA in economics and political science from Furman University and is a PhD candidate in economics at George Mason University.

Keywords: Internet security, cybersecurity, Internet governance, indirect liability, malware, informal institutions, Internet service providers, law and economics, legal polycentrism, legal institutions, legal pluralism

JEL codes: L86, K13, D02, K42

Abstract

Lichtman and Posner argue that legal immunity for Internet service providers (ISPs) is inefficient on standard law and economics grounds. They advocate indirect liability for ISPs for malware transmitted on their networks. While their argument accurately applies the conventional law and economics toolkit, it ignores the informal institutions that have arisen among ISPs to mitigate the harm caused by malware and botnets. These informal institutions carry out the functions of a formal legal system—they establish and enforce rules for the prevention, punishment, and redress of cybersecurity-related harms.

In this paper, I document the informal institutions that enforce network security norms on the Internet. I discuss the enforcement mechanisms and monitoring tools that ISPs have at their disposal, as well as the fact that ISPs have borne significant costs to reduce malware, despite their lack of formal legal liability. I argue that these informal institutions perform much better than a regime of formal indirect liability. The paper concludes by discussing how the fact that legal polycentricity is more widespread than is often recognized should affect law and economics scholarship.

Internet Security without Law: How Service Providers Create Order Online

Introduction

Computer viruses cause a great deal of harm. They steal money from users' bank accounts, distribute spam email from infected machines, and self-organize into botnets that can be used to temporarily overwhelm websites and other servers. Undesirable though these malicious programs may be, they are also costly to avoid, detect, and deter. Because costs are imposed both by the malicious programs themselves and by their abatement, economic analysis needs to be brought to bear to determine the kinds of policy responses that may be appropriate. Some authors have attempted to do this.[1]

In one important paper on the subject, Lichtman and Posner argue that recent trends in the courts and Congress toward complete immunity for Internet service providers (ISPs) for their role in the propagation of malicious computer code (malware) are economically inefficient.[2] They argue that ISPs should face indirect liability for the damage caused by malware, both on policy grounds and by tort law principles.[3] Although their argument is otherwise very thorough, it omits the fascinating role of informal institutions among ISPs that have arisen to deal with the problem of malware.

This omission is significant but understandable. Conventional economic analysis has often assumed that the legal system is formal and monocentric, that law is made

[1] Michel J. G. van Eeten and Johannes M. Bauer, "Economics of Malware: Security Decisions, Incentives and Externalities" (STI Working Paper 2008/1, OECD Directorate for Science, Technology, and Industry, 2008), http://www.oecd.org/dataoecd/53/17/40722462.pdf; Michel Van Eeten and Johannes M. Bauer, "Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications," *Journal of Contingencies and Crisis Management* 17 (December 2009): 221–32; and Eli Dourado, "Is There a Cybersecurity Market Failure?" (working paper, Mercatus Center at George Mason University, 2011), http://mercatus.org/sites/default/files/publication/Cybersecurity_Dourado_WP1205_0.pdf.

[2] Doug Lichtman and Eric Posner, "Holding Internet Service Providers Accountable," *Supreme Court Economic Review* 14 (2006): 221–60.

[3] Ibid., 221, and throughout.

explicitly and solely by the government. Increasingly, many economists and legal scholars have recognized that this assumption is unwarranted.[4] They have begun to study the ways in which informal, nonstate institutions govern individual behavior.[5] These informal institutions carry out the functions of formal legal systems—they establish and enforce rules for the prevention, punishment, and redress of harms—even as they lack formal systems' threat of violence as an enforcement mechanism.

I argue that the informal institutions that enforce network security norms between ISPs are more efficient than the hypothetical formal legal regime Lichtman and Posner propose. Indeed, because formal and informal enforcement of security norms are substitutes, not complements,[6] the formal legal system's neglect of ISPs is not merely benign but has also helped the Internet to flourish. The paper proceeds as follows. In the next section, I discuss Lichtman and Posner's argument and the underlying conventional theory in more detail. In section three, I document the informal rules and enforcement mechanisms that limit the propagation of malware on the Internet to approximately efficient levels. In the fourth section, I compare the outcome under the existing system to the probable outcome under a regime of indirect liability enforced by formal law and demonstrate that these two regimes are incompatible. In conclusion, I discuss the implications of this case for other policy analyses and for law and economics generally.

[4] Lessig argues that in addition to formal law, norms, markets, and "architecture" also regulate human behavior. See Lawrence Lessig, "The New Chicago School," *Journal of Legal Studies* 27, no. S2 (June 1998): 661–91. He argues that code is the dominant regulator in cyberspace. See Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006). Shavell discusses morality as a regulator of conduct separate from formal law. See Steven Shavell, "Law versus Morality as Regulators of Conduct," *American Law and Economics Review* 4, no. 2 (Fall 2002): 227–57.

[5] See Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge, UK: Cambridge University Press, 1990); and Robert Ellickson, *Order without Law: How Neighbors Settle Disputes* (Cambridge, MA: Harvard University Press, 1991).

[6] This claim is substantiated in section four.

The Conventional Analysis of ISP Security

Lichtman and Posner accurately summarize the conventional economic analysis of indirect liability and apply it to the case of malware transmission.[7] Indirect liability, by way of definition, "is said to attach in instances where the law holds one party liable because of a wrong committed by another."[8] They identify four factors that make the assignment of indirect liability as a default rule desirable: (1) the direct actors are to some extent beyond the reach of law, (2) transaction costs prevent the assignment of liability by contract to the efficient bearer, (3) someone else is in a position to prevent the harm caused by the direct actor, and (4) someone else will select a level of activity that is too high unless made to account for the negative externalities generated by the activity.[9]

The first two factors are extremely important; at least one of them must hold for indirect liability to be plausibly efficient. If direct actors—those that directly create the harm—are subject to the effective reach of law and transaction costs are sufficiently low, then the Coase Theorem applies and the default liability rule is economically unimportant.[10] Liability can be assigned by contract where it is most efficiently borne. The latter two factors can be thought of as helpful but not dispositive guidelines to identify the cases in which the imposition of indirect liability may be useful.

Lichtman and Posner document the ways in which malware transmission on the Internet conforms to the conventional argument for indirect liability. First, the relevant bad actors are beyond the effective reach of law. Malware coders, those ultimately

[7] Lichtman and Posner, "Holding Internet Security Providers Accountable," 228–40.
[8] Ibid, 228. "Indirect liability" is a generic phrase that encompasses other terms such as vicarious liability, secondary liability, and third-party liability.
[9] Ibid., 229–33.
[10] Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3 (October 1960): 1–41. Coase shows that the default legal rule affects economic efficiency only if it is too costly to write a contract to achieve the efficient solution or if property rights are not well defined. Lichtman and Posner, "Holding Internet Security Providers Accountable," 229, note some second-order constraints.

responsible for the theft and disruption caused by their programs, are very difficult to identify.[11] Even if they can be identified, they may live overseas, so their civil or criminal liability would raise international jurisdictional issues.[12] Finally, even if they could be identified and brought to justice, it is unlikely many malware coders have the resources to pay for the losses they generate; they are judgment proof.[13] The other direct actors involved, ordinary Internet users who do not take adequate security precautions, may be identifiable, but it is nevertheless difficult and costly to apportion liability among them.[14]

Second, transaction costs prevent ISPs from efficiently assigning liability to each other by contract. Lichtman and Posner argue that peering arrangements—agreements between ISPs to exchange Internet traffic—could not form the basis of a Coasian resolution of the malware problem.

> Any network of contracts focusing on issues of cybersecurity would be perpetually out of date, and updating such a complicated web of interdependent security obligations would be all but impossible given the number of parties involved and the complicated questions any update would raise regarding appropriate adjustments to the flow of payments.[15]

Third, ISPs are in a position to detect and curtail malware transmission. "An ISP can detect criminal behavior by analyzing patterns of use, much as a bank can detect credit card theft by monitoring each customer's pattern of purchases."[16] Lichtman and Posner also propose that ISPs could record and store each user's data stream for some

[11] Ibid., 233–34.
[12] Ibid., 234.
[13] Ibid.
[14] Ibid., 234–35.
[15] Ibid., 235–36.
[16] Ibid., 236–37.

period of time, notwithstanding the high volume of communications.[17] In any case, technologies that identify infected users are available and in use.[18]

Lichtman and Posner do not rely as much on the fourth factor they identify, the internalization of unavoidable externalities in the activity level.[19] In principle, when some activity unavoidably harms innocent bystanders, a more economically efficient outcome can be achieved by imposing a cost on those who are in a position to decide how much of the activity to pursue.[20] When made to account for the harms they are inflicting on others, they will do less of it. If ISPs were liable for the transmission of malware across their networks, they would bear losses that would raise their costs. The price of Internet access would rise, and the quantity of Internet use—as well as the amount of unavoidable malware transmission—would fall. However, Lichtman and Posner note that there are also positive externalities associated with Internet access, and they do not want to penalize negative externalities without rewarding positive ones.[21] In addition, forcing ISPs to internalize malware externalities could have the side effect of discouraging consumer self help, such as installing antivirus software.[22]

The "activity level" rationale aside, Lichtman and Posner have built a strong conventional law and economics argument in favor of indirect liability in this setting. If the conventional account is correct, then we should expect, in the absence of indirect liability, that ISPs would not take very many steps to detect and prevent malware transmission and that the level of malware-related harm would be inefficiently high. We

[17] Ibid., 237.
[18] Some of these are discussed in section three.
[19] Lichtman and Posner, "Holding Internet Security Providers Accountable," 238.
[20] Ibid., 231.
[21] Ibid., 238–39.
[22] Ibid., 239.

can observe whether ISPs make efforts to ameliorate the negative effects of malware, but we cannot directly observe whether those efforts result in an economically efficient outcome. Economists make what are ultimately intuitive judgments about efficiency by evaluating the incentives the participants involved in making decisions face. Lichtman and Posner's judgment that the level of malware-related harm is inefficiently high is based on their study of ISPs' incentives with respect to the formal legal system, but to perform a complete evaluation we must turn to the role of the informal institutions that restrain malware.

How ISPs Enforce Security Norms

State-produced and state-enforced law governs many of our physical interactions, but it has a much weaker role with respect to Internet security. As Mueller writes, "If we look at how security is actually produced, we discover that most of the actual work is done not by national states promulgating and enforcing public law, but by private actors in emergent forms of peer production, network organizations, and markets."[23] States do have a role in producing Internet security, but it is the role of a peer, not of a master. Mueller writes,

> Security governance in cyberspace takes place mainly through informal, trust-based relationships among the Internet operational community members. These can be characterized as network forms of organization or as a kind of peer production or both. States are players in these arrangements, but are rarely in a position to exert hierarchical power.[24]

To understand how security is produced in a nonhierarchical manner, it is important to understand how the Internet is constituted and the features of that

[23] Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: Massachusetts Institute of Technology, 2010), 160–61.
[24] Ibid., 163.

constitution that enable enforcement of security norms. The Internet is a network of separately administered networks. As of April 29, 2012, there are 40,957 autonomous systems (ASes) in the Internet's routing system.[25] Some of these ASes are small and connected to as few as one other AS; others are very large and connected to hundreds of other ASes.[26] The connections between ASes take two forms: commercial arrangements in which one AS pays another to carry its traffic are called *transit* agreements, while unpriced connections between ASes are called *peering* agreements.[27] Transit agreements are common near the edge of the Internet, while peering agreements are more common near the core.[28]

Woodcock and Adhikari analyze 142,210 peering agreements representing 86 percent of the world's Internet carriers and find that over 99.5 percent of them are informal, "handshake" agreements.[29] "The common understanding is that only routes to customer networks are exchanged, that BGP [Border Gateway Protocol, which announces what network destinations are reachable via the connection] version 4 is used to communicate those routes, and that each network will exercise a reasonable duty of care in cooperating to prevent abusive or criminal misuse of the network."[30] Public Internet exchange points (IXPs) provide a physical, and in some cases, a social medium for peering. Some commercial, carrier-neutral IXPs have been known to arrange social events for network operators to get to know each other in order to encourage new peering.

[25] Tony Bates, Philip Smith, and Geoff Huston, "CIDR Report," April 29, 2012, http://www.cidr-report.org/as2.0. An autonomous system may be composed of more than one network, but it presents a common routing policy to the rest of the Internet.
[26] Ibid.
[27] Bill Woodcock and Vijay Adhikari, "Survey of Characteristics of Internet Carrier Interconnection Agreements," Packet Clearing House, May 2, 2011, http://www.pch.net/resources/papers/peering-survey/PCH-Peering-Survey-2011.pdf.
[28] Ibid.
[29] Ibid.
[30] Ibid.

Because the vast majority of peering agreements are informal, at-will arrangements, if one party is unhappy with another's security practices or responsiveness to complaints, it can unilaterally terminate the agreement and depeer. Depeering is the ultimate enforcement mechanism used by ISPs against negligent or willfully insecure networks. It is a punishment that in fact gets used, because it can be profitable to run a network that welcomes cybercriminals. Service providers that tolerate complaint-generating customers are known as bulletproof hosts. They can charge up to ten times more for their services than hosting companies that cooperate with the community's security norms because cybercriminals are willing to pay a premium to be able to stay in business.[31] A vivid example of depeering as an enforcement mechanism is provided by the case of McColo, a California-based bulletproof web host.

In 2008, *Washington Post* investigative reporter Brian Krebs conducted a four-month investigation of McColo.[32] He talked with network security experts and amassed evidence that McColo was the host for "some of the most disreputable cyber-criminal gangs in business today."[33] In November 2008, Krebs contacted McColo's two major upstream providers, Global Crossing and Hurricane Electric, and showed them his evidence. These upstream firms had little choice but to sever the relationship or risk being depeered. "Global Crossing . . . declined to discuss the matter, except to say that Global Crossing communicates and cooperates fully with law enforcement, their peers, and security researchers to address malicious activity."[34] A spokesman for Hurricane

[31] Brian Krebs, "Shadowy Russian Firm Seen as Conduit for Cybercrime," *Washington Post*, October 13, 2007.
[32] Brian Krebs, "Major Source of Online Scams and Spams Knocked Offline," *Security Fix* Blog, November 11, 2008, http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html.
[33] Brian Krebs, "Host of Internet Spam Groups Is Cut Off," *Washington Post*, November 12, 2008.
[34] Ibid.

Electric reports, "We looked into it a bit, saw the size and scope of the problem [the *Washington Post* was] reporting and said 'Holy cow!' Within the hour we had terminated all of our connections to them."[35] Because McColo was the host for the command and control server of the Srizbi botnet, among others, the global volume of email spam fell by about two-thirds nearly instantly.[36] Furthermore, online retail fraud plummeted from nearly $250,000 per day to nearly zero.[37]

In addition to possessing effective enforcement mechanisms, the Internet community has invested a great deal in monitoring capabilities. Mueller writes,

> Interpersonal and organizational networks among Internet service providers (ISPs), computer security incident response teams (CSIRTs or CERTs), domain name registrars, hosting companies, email-based expert discussion forums, the information technology departments of major user organizations and government agencies, and a burgeoning market for private security services bear the brunt of the burden of protecting networks. These communities are not coterminous with national boundaries and their transnational nature can be viewed as responses to the limitations and obstacles of territorial law enforcement. The procedures used are heavily reliant on the Internet itself and on computationally enabled analytical tools to monitor incidents, identify problems, communicate among the parties, and formulate and implement responses.[38]

The basic monitoring institution on the Internet is the computer security incident response team (CSIRT, or sometimes CERT, for computer emergency response team). A CSIRT is a team of technical experts that monitors traffic, identifies threats and vulnerabilities, and formulates solutions to security problems. In 1988, in response to the

[35] Ibid.
[36] Ibid.
[37] Brian Krebs. "Retail Fraud Rates Plummeted the Night McColo Went Offline," *Security Fix* Blog, December 11, 2008, http://voices.washingtonpost.com/securityfix/2008/12/mccolo_shutdown_killed_retaile.html.
[38] Mueller, *Networks and States*, 163.

Morris worm, one of the first pieces of malware to be distributed online,[39] DARPA funded the establishment of the CERT Coordination Center (CERT-CC) at Carnegie Mellon University.[40] True to its name, CERT-CC facilitates coordination and communication between CSIRTs around the world and supplies development and training materials to those who wish to start new CSIRTs. Virtually any Internet stakeholder can start a CSIRT. Some are located at universities or private companies; others are run by governments. Figure 1 shows a map of CSIRTs around the world.

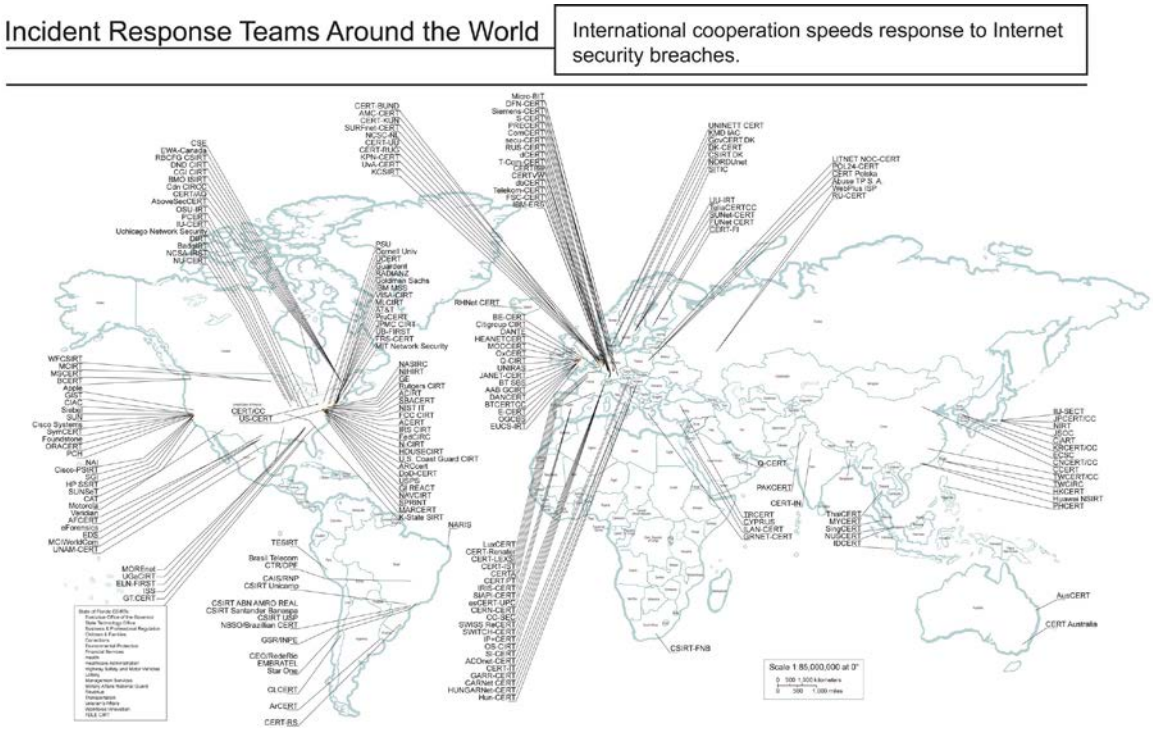

Figure 1

Source: "Internet Response Teams around the World," CERT, Software Engineering Institute, Carnegie Mellon University, updated January 12, 2012, http://www.cert.org/csirts/csirt-map.html.

In addition to the expertise of the team members and of CERT-CC, CSIRTs benefit from security tools provided by the private sector. Many familiar companies that

[39] Thomas A. Longstaff et al., "Security of the Internet," in *The Froehlich/Kent Encyclopedia of Telecommunications* 15, ed. Fritz E. Froehlich and Allen Kent (New York: Marcel Dekker, 1997),231–55, http://www.cert.org/encyc_article/tocencyc.html.
[40] Ibid.

provide consumer-grade security products also create products for CSIRTs and network operators. Other companies, such as FireEye, specialize solely in malware and combating botnets. Still other companies design custom tools for CSIRTs to monitor their networks more effectively.

CSIRTS and ASes also have an important tool provided by the nonprofit sector. In 1994, West Coast ISPs founded Packet Clearing House, a nonprofit research institute that has since established one-third of the world's IXPs.[41] It performs numerous projects in support of the Internet community, such as studying Internet topology[42] and running an IXP directory.[43] It also supplies a secure and authenticated communications platform called INOC-DBA (Inter-Network Operations Center Dial-By-ASN).[44] An operator of one AS who notices suspicious traffic originating from another AS can dial the appropriate five-digit registered AS number and immediately be connected with that AS's network operations center. This direct connection between technical staff facilitates rapid cooperation. Other critical individuals, such as in the policy and vendor communities, are also reachable through this system. "In January of 2003, the INOC-DBA phone system became the first single telephone network of any sort to reach all seven continents."[45]

The monitoring tools that have been developed by the Internet technical community are well suited to its needs:

> The common denominator of these efforts is that they are predicated on the need for rapid action informed by specialized technical expertise; the

[41] Tekla S. Perry, "Bill Woodcock: On an Internet Odyssey." *IEEE Spectrum*, February 2005, http://spectrum.ieee.org/computing/networks/bill-woodcock-on-an-internet-odyssey/0.
[42] Packet Clearing House, "Research," http://www.pch.net/purpose/research.php.
[43] Packet Clearing House, "Internet Exchange Directory," https://prefix.pch.net/applications/ixpdir/.
[44] Packet Clearing House, "INOC-DBA," http://www.pch.net/inoc-dba/.
[45] Gaurab Raj Upadhaya. "INOC-DBA SIP Proxy FAQ," Packet Clearing House, http://www.pch.net/inoc-dba/docs/inoc-dba-sip-conf-faq.txt.

> need for close cooperation across multiple organizational and jurisdictional boundaries; and direct operational control of some form of access to the Internet (e.g., servers, bandwidth, domain names).[46]

The system empowers the engineers responsible for making the Internet work, while keeping obstacles to their important work to a minimum.

A combination of good incentives enabled by the threat of depeering and good monitoring capabilities, developed by Internet stakeholders, has resulted in substantial efforts on the part of ISPs to address their customers' malware infections. It is perhaps surprising to many that this is so. In 2007, the House of Lords reported,

> At the moment, although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so. Indeed, there is a disincentive, since customers, once disconnected, are likely to call help-lines and take up the time of call-centre staff, imposing additional costs on the ISP.[47]

Van Eeten and Bauer conduct in-depth interviews on malware with networked computer organizations and find that

> All ISPs we interviewed described substantial efforts in the fight against malware, even though they are operating in highly competitive markets and most countries do not have governmental regulations requiring them to do so. All of them were taking measures that were unheard of only a few years ago. Most of the interviewees dated this change to around 2003, when it became obvious that it was in the ISPs own interest to deal with end user insecurity, even though legally it was not their responsibility.[48]

Michael O'Reirdan, chairman of the Messaging Anti-Abuse Working Group—composed of ISPs, email providers, and security vendors—says, "All over the U.S., ISPs

[46] Mueller, *Networks and States*, 164.
[47] UK House of Lords, Science and Technology Committee, 5th Report of Session 2006–2007, *Personal Internet Security, Volume I: Report* (London: House of Lords, August 10, 2007), 30, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf.
[48] Michel Van Eeten and Johannes M. Bauer, "Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications," *Journal of Contingencies and Crisis Management* 17 (December 2009): 225.

currently have notification systems in place to tell their users they are infected and—whether they deliver these warnings via email, phone, walled gardens, or inline warnings—the warnings are being delivered."[49] These notifications raise ISPs' support costs; the fact that ISPs are willing to bear these costs despite the lack of formal legal liability is evidence that there is a significant amount of informal enforcement of security norms. These norms have been articulated by multiple organizations within the Internet technical community, and the Internet Engineering Task Force has published best practices for mitigating bot activity and harm.[50]

Informal Enforcement versus Formal Law

The informal institutions outlined in the previous section do not achieve perfect security, nor would it be economically efficient for them to do so. Security is costly and perfect security is prohibitively so. We should increase security if the marginal benefits of additional security are higher than the marginal costs, but at some point the marginal costs of security exceed the marginal benefits. Some level of insecurity is therefore associated with economic efficiency. I do not claim that these institutions are efficient in a first-best sense. Mueller agrees: "Legitimate questions about the overall effectiveness of current methods are often raised and many proposals for improvement are worth considering." [51] However, there is a strong case to be made that these evolved, noncoercive institutions outperform a hypothetical indirect liability regime supported by

[49] Kelly Jackson Higgins, "ISP Backlash over Feds' Bot Notification Initiative," *Dark Reading* (October 5, 2011), http://www.darkreading.com/insider-threat/167801100/security/client-security/231900078/isp-backlash-over-feds-bot-notification-initiative.html.
[50] J. Livingood, N. Mody, and M. O'Reirdan, "Recommendations for the Remediation of Bots in ISP Networks," IETF Request for Comments 6561, March 2012, http://www.ietf.org/rfc/rfc6561.txt.
[51] Mueller, *Networks and States*, 164.

formal state-based law as Lichtman and Posner advocate. There are a number of reasons to prefer the status quo.

First, the at-will, informal nature of peering agreements gives network operators flexibility to determine what constitutes due care in a dynamic environment. Formal legal standards of care may not be able to adapt as quickly as needed to rapidly changing circumstances. A vivid example of the dynamic nature of the malware threat is provided by changes in the architecture of botnet command and control structures. Prior to 2007, malware was engineered to direct infected computers to contact a centralized command and control server, utilizing the IRC protocol or HTTP.[52] To disable a botnet, security researchers would capture a copy of the virus, analyze its communications, and identify the central command and control server.[53] Once the command and control server was identified, it could be physically disabled by law enforcement or the ISP that hosted it,[54] or the ISP that hosted the server could be depeered by its upstream providers, as McColo was for hosting the Srizbi command and control server.[55] However, in 2007, malware coders innovated by introducing the Storm Worm, which created a botnet based on a peer-to-peer design. The Storm botnet did not have a centralized command and control server.[56] This innovation affects the efficient standard of care for ISPs. Prior to Storm, network operators may have felt that their peers were exercising a reasonable duty of care if they disconnected command and control servers once they were detected. However, in the new environment, as malware coders adopt the new strategy, such care may be less

[52] Thorsten Holz, Moritz Steiner, Frederic Dahl, Ernst Biersack, and Felix Freiling, "Measurements and Mitigation of Peer-to-Peer-Based Botnets: A Case Study on Storm Worm" (working paper, University of Mannheim and Institut Eurécom, Sophia Anttipolis, 2008), http://pi1.informatik.uni-mannheim.de/filepool/publications/storm-leet08.pdf.
[53] Ibid.
[54] Ibid.
[55] Krebs, "Host of Internet Spam Groups Is Cut Off."
[56] Holz, et al. "Measurements and Mitigation of Peer-to-Peer-Based Botnets."

important to network operators; they may value other forms of cooperation more highly, such as notifying infected customers and bearing the associated higher support costs. This may explain why ISPs have in fact relied more on customer bot notification in recent years. Informal enforcement of cooperative norms means that standards of care can rapidly adapt to dynamic circumstances.

Second, formal legal proceedings are adversarial and could reduce ISPs' incentives to share information and cooperate. Because the informal institutions do not include adversarial evidentiary hearings, there is little incentive to hold back information, at least to the extent that it does not violate the law by exposing private customer information. If ISPs feared that the information they shared could be used against them in court, information would need to go through an internal legal review before it could be shared. Even if courts attempt to offset this by ignoring evidence generated through antimalware cooperation, it still raises new strategic considerations in sharing information. Given the importance of information sharing between ISPs and other members of the Internet technical community, introducing adversarial proceedings could reduce the security of the Internet.

Third, the direct costs of going to court can be substantial, as can be the time associated with a trial. Under the status quo, however, ISPs do not need to go to court to enforce security norms. Security concerns are addressed quickly or punishment—depeering—is imposed rapidly. Lichtman and Posner suggest that ISPs could be required to record the data stream for each of their subscribers,[57] which would be extremely

[57] Lichtman and Posner, "Holding Internet Service Providers Accountable," 237.

costly.[58] Status quo institutions avoid these substantial costs, and do not, in addition, raise the privacy concerns associated with storing subscriber data streams.

Fourth, international cooperation between state-based legal systems is limited. Lichtman and Posner acknowledge this, but they argue that imperfect cooperation is better than none and that good policy in the United States can influence policy in other jurisdictions.[59] However, because Lichtman and Posner do not consider existing informal institutions as a competing legal system, they do not acknowledge that under the status quo, international cooperation is strong. Because existing institutions match the topology of the Internet rather than that of the political system, they are better suited to enforcing security norms on the Internet.

Finally, many ISPs and ASes are small and subject to limited liability, which may prevent injured parties from collecting damages from them.[60] This fact undermines one of the central arguments for indirect liability, "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*."[61] Indeed, some cyber-criminals may have deeper pockets than the ISPs that might be found liable under a regime of indirect liability. For example, a 2007 report about the Russian Business Network, a

[58] According to an estimate by Cisco from 2011, global IP traffic in 2012 exceeds one exabyte per day and is expected to more than double by 2015. If the statute of limitations were as short as one year, ISPs would need to store more than 400 exabytes of data in 2012 alone. Assuming that hard drives can be purchased for $50 per terabyte, this would be a $20 billion expense just for the physical storage medium., "Cisco Visual Networking Index: Forecast and Methodology, 2010–2015," (white paper, Cisco, June 1, 2011), http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html.

[59] Lichtman and Posner, "Holding Internet Security Providers Accountable," 246–248.

[60] Of the 40,957 ASes in the routing system as of April 29, 2012, 17,105 announce only one routing prefix, which is evidence that they are probably small firms. Many more announce only a few routing prefixes. In comparison, BellSouth.net, one of AT&T's several networks, announces 3,424 routing prefixes. See Bates, Smith, and Huston, "CIDR Report."

[61] Lichtman and Posner, "Holding Internet Security Providers Accountable," 222, emphasis added.

group "linked to around 60% of all cybercrime," alleged that its 24-year-old founder, known only as Flyman, was the nephew of an influential Russian politician.[62] Even if Flyman is not a Russian oligarch, he could have more assets than the thousands of tiny ISPs that help compose the Internet, which undercuts the case for indirect liability in this context. More significantly, to deal with the apportionment of liability, Lichtman and Posner suggest that ISPs could face joint and several liability.[63] This could have an unwelcome chilling effect on peering between ISPs of different means. Deep-pocketed firms are not likely to want to peer with judgment-proof ones if in so doing they will become, in practice, wholly liable for the latter's actions. Since promiscuous peering is the *sine qua non* of the Internet, joint and several indirect liability could have a radical effect on how the Internet is constituted.

As several of the arguments above indicate, indirect liability and the informal institutions currently in place are more substitutes than complements. Informal, at-will peering arrangements are possible because ISPs anticipate that an unresolvable security dispute will merely result in depeering, not litigation. Unless the court is able to dynamically articulate a highly efficient liability standard, the vast majority of ISPs would be forced, for the first time, to turn to formal contracts to define their expectations and duties with respect to cybersecurity, which by Lichtman and Posner's own admission "would be perpetually out of date."[64] The introduction of indirect liability would change ISPs' calculus with respect to both what information to share and with whom to peer.

[62] Peter Warren, "Hunt for Russia's Web Criminals," *The Guardian* (London), November 14, 2007, http://www.guardian.co.uk/technology/2007/nov/15/news.crime.
[63] Lichtman and Posner, "Holding Internet Security Providers Accountable," 246.
[64] Lichtman and Posner, "Holding Internet Security Providers Accountable," 235.

These changes would tend to undermine, if not completely destroy, the informal institutions that currently enforce norms.

It is impossible to make a direct comparison between the status quo and a nonexistent regime of indirect liability enforced by formal law, but all things considered, current institutions perform reasonably well. As I have argued, formal legal rules would be less dynamic, induce less cooperation, raise costs, be less effective internationally, and limit peering, especially for smaller ISPs. Even if current institutions are not efficient in a first-best sense, they may be more efficient than other institutions actually in our opportunity set. Those who propose alternative institutions must show that their proposals compare favorably with the status quo. Lichtman and Posner doubt that current formal legal intervention is adequate to deal with the problem of malware, but by failing to adequately consider the benefits of existing informal institutions, they have not shown that their proposal for indirect liability would improve economic efficiency.

Discussion: Law, Economics, and Polycentricity

Law and economics has been dominated by the Coasian paradigm that when transaction costs are low and property rights are well defined, the default legal rule does not matter. When those conditions do not hold, economic analysis is used to determine what the default legal rule should be. This approach has yielded many advances, but in some cases it can lead one astray. Human activity is constrained by informal institutions as well as formal law, and these institutions carry out many of the same functions as state-based legal systems. In some cases, they do so even when formal transaction costs are high or property rights are poorly defined. As the informal enforcement of security

norms between ISPs shows, our legal regime is more polycentric than many legal scholars have recognized.

An advantage of the Coasian paradigm is that it is easy to apply. It is much more difficult to assess whether a particular problem could be resolved through informal institutions, or whether existing nonstate institutions adequately address a problem. There is no simple rubric. Consequently, to evaluate a legal problem from a polycentric perspective, legal scholars will need to become much more familiar with the particulars of the institutions and domains they are investigating. The fact that the polycentric approach demands a fair amount of subject-matter expertise perhaps explains why legal scholars have stuck to the much simpler Coasian rubric.

Despite the lack of a clear-cut guide to the application of polycentric legal principles, political scientists and economists have conducted much research evaluating institutions that govern common pool resources (CPRs). This research program has been centered on the Bloomington school of political economy. Ostrom synthesizes and summarizes some of its major findings.[65] She argues that there are a number of design principles that seem to be common among successful CPR institutions. These principles are listed in table 1 and form a good starting point for analysis of informal legal institutions.

Table 1. Design Principles Illustrated by Long-Enduring CPR Institutions

1.	Clearly defined boundaries Individuals or households who have rights to withdraw resource units from the CPR must be defined, as must the boundaries of the CPR itself.
2.	Congruence between appropriation and provision rules and local conditions Appropriation rules restricting time, place, technology, and/or quantity of resource units are related to local conditions and to provision rules requiring labor, material, and/or money.

[65] Ostrom, *Governing the Commons*.

3. Collective-choice arrangements
   Most individuals affected by the operational rules can participate in modifying the operational rules.
4. Monitoring
   Monitors, who actively audit CPR conditions and appropriator behavior, are accountable to the appropriators or are the appropriators.
5. Graduated sanctions
   Appropriators who violate operational rules are likely to be assessed graduated sanctions (depending on the seriousness and context of the offense) by other appropriators, by officials accountable to these appropriators, or by both.
6. Conflict-resolution mechanisms
   Appropriators and their officials have rapid access to low-cost local arenas to resolve conflicts among appropriators or between appropriators and officials.
7. Minimal recognition of rights to organize
   The rights of appropriators to devise their own institutions are not challenged by external governmental authorities.

For CPRs that are part of larger systems:

8. Nested enterprises
   Appropriation, provision, monitoring, enforcement, conflict resolution, and governance activities are organized in multiple layers of nested enterprises.

Source: Ostrom, *Governing the Commons*, 90.

The possibility that informal institutions could effectively solve legal problems strengthens the case for a presumption of state noninterference relative to conventional law and economics analysis. State interference could have the unintended consequence of destroying the mechanisms by which legal problems are in fact remedied, often at lower cost than the state-based legal regime could achieve. Voluntary solutions are often highly effective, even when transaction costs are high and property rights are imperfectly defined. Consequently, legal scholars should increasingly view the state as the arbiter of last resort, rather than as the sole provider of legal services. This is especially true in the domain of cybersecurity, which has robust informal institutions that likely outperform formal legal intervention.