Pace Law Review

Volume 34
Issue 2 *Spring 2014*

Article 3

April 2014

Global Cyber Intermediary Liability: A Legal & Cultural Strategy

Jason H. Peterson
Sawyer Business School, Suffolk University

Lydia Segal
Sawyer Business School, Suffolk University

Anthony Eonas
Sawyer Business School, Suffolk University

Global Cyber Intermediary Liability: A Legal & Cultural Strategy

Jason H. Peterson,* Lydia Segal, and Anthony Eonas*****

I. Introduction

Cybercrime is one of the most serious problems facing modern economies around the world.[1] In the United States alone cybercrime cost an estimated $9 billion in 2011.[2] In Germany, it cost about $6 billion that year.[3]

Reformers have poured a great deal of effort into trying to figure out what to do about the problem.[4] Scholars have written

* Assistant Professor of Business Law & Ethics, Sawyer Business School, Suffolk University, Boston, MA.

****** Associate Professor of Business Law & Ethics, Sawyer Business School, Suffolk University, Boston, MA.

******* Associate Professor of Business Law & Ethics, Sawyer Business School, Suffolk University, Boston, MA.

1. *See* PONEMON INSTITUTE, 2012 COST OF CYBER CRIME STUDY: UNITED STATES 1-2 (2012), http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf; *see also* Charlotte Decker, *Cybercrime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 961-62 (2008).

2. PONEMON INSTITUTE, *supra* note 1, at 2; *see also* Sara Yin, *Cyber Crime Costs Jump 56 Percent*, PC MAG. (Aug. 3, 2011, 2:45 PM), http://www.pcmag.com/article2/0,2817,2390371,00.asp.

3. PONEMON INSTITUTE, *supra* note 1, at 2.

4. *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659 (2005); Decker, *supra* note 1, at 963; Salil K. Mehra, *Law and Cybercrime in the United States Today*, 58 AM. J. COMP. L. 659 (2010); Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237 (2000); Meiring de Villiers, *Enabling Technologies of Cyber Crime: Why Lawyers Need to Understand It*, 11 U. PITT. J. TECH. L. & POL'Y 4 (2011); Jonathan B. Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals with Old Laws and Little Money*, 28 AM. J. CRIM. L. 95 (2000).

about it extensively and put forth multiple proposals for change.[5] So far, however, little seems to be making a dent.[6] In fact, cyber-attacks are becoming more frequent, more vicious, and more expensive every year.[7]

One reason for the lack of an effective solution may be that scholars and experts are focused almost entirely on cybercriminals and the countries that support their crimes.[8] They seem to be largely ignoring the critical role played by intermediaries, which include both Internet Service Providers (ISPs) and hosts, in facilitating cybercrime.[9] ISPs provide the actual gateway for users to the Internet, while hosts provide server space to users.[10] Some intermediaries provide both functions.[11] A search of law reviews reveals no recent articles considering policy changes geared towards ISP liability as means to combat cybercrime and a complete disregard for the role of hosts.

On the one hand, this lack of attention to ISPs and failure to spotlight their strategic relationships to hosts are astonishing because hosts and ISPs provide the means and venue for cybercriminals to operate. On the other hand, the lack of attention is understandable because hosts and ISPs operate in a virtual no-man's land in terms of laws, legislation, and even national jurisdiction.[12] This is in spite of the

5. *See* sources cited *supra* note 4.

6. *See* Decker*, supra* note 1, at 961-62.

7. *See* PONEMON INSTITUTE, *supra* note 1, at 2; *see also* Yin*, supra* note 2 (discussing the challenge of determining the cost of cybercrime). The median annual cost of cybercrime for organizations in 2011 was $5.9 million, which represented a 56 percent annual increase. Yin*, supra* note 2. The components of loss include: (1) intellectual property; (2) direct financial; (3) sensitive information; (4) opportunity costs; (5) recovery costs; and (6) reputation. *Id.*; *see also* Decker, *supra* note 1, at 963 (noting cybercrime results in billions of annual losses).

8. *See* sources cited *supra* note 4.

9. *See id.*

10. *See* Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 256 (2005); *see also* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 613-15 (E.D. Pa. 2004).

11. *See Pappert*, 337 F. Supp. 2d at 613-15; Mann & Belzley, *supra* note 10, at 256.

12. *See* Mann & Belzley, *supra* note 10, at 244.

important regulatory function ISPs play online.[13]

This Article fills the gap in the debate on fighting cybercrime. It considers the role of intermediaries and the legal and cultural strategies that countries may adopt. Part II.A of this Article examines the critical role of intermediaries in cybercrime. It shows that the intermediaries' active participation by facilitating the transmission of cybercrime traffic removes a significant barrier for individual perpetrators. Part II.B offers a brief overview of legal efforts to combat cybercrime, and examines the legal liability of intermediaries in both the civil and criminal context and in varying legal regimes with an emphasis on ISPs. Aside from some level of injunctive relief, intermediaries operate in a largely unregulated environment. Part III looks at what we can learn from other countries. The cleanest intermediary country, Finland, and the worst country, Lithuania, were selected in order to explore the causes for the differences between country performances. The section examines the remarkable distinctions between national cultures to explain differences in national cybercrime rates.

Part III.A of this Article argues that the criminal code laws do not account for the difference in host and ISP performances between Finland and Lithuania. There are few differences in the codified laws pertaining to cybercrime between these countries. Instead, it is Finland's cultural and business environments that appear to drive its cybercrime ranking. Part IV suggests reforms to shift a country's culture to make it less prone to corruption. However, changing a culture takes time so Part IV also proposes a private law scheme in which intermediaries are unable to wave the "flag of immunity," as they do now. The guiding philosophy for this proposal is that harmed parties should be permitted to recover damages directly from "bad" intermediaries.

13. *See* Sandra Braman & Stephanie Lynch, *Advantage ISP: Terms of Service as Media Law*, *in* RETHINKING RIGHTS AND REGULATIONS 249, 250-51 (Lorrie Faith Cranor & Steven S. Wildman eds., 2003).

II. Intermediaries

A. *Intermediaries and Cybercriminals*

Cybercriminals do not operate within a vacuum.[14] The Internet's framework consists of a handful of intermediaries, each with its own relationship with the cybercriminal.[15] For example, an individual who creates and releases a Trojan in Lithuania relies upon a handful of participants.[16] Figure 1 provides a simplified view of the relationships of several intermediaries, including registration companies, hosting companies and Internet Service Providers (ISPs). Registration companies provide website domain names to Internet users.[17] Hosting firms sell server space and provide IP addresses to those who wish to access the Internet.[18] ISPs provide the actual gateway to the Internet for the Lithuanian perpetrator.[19]

14. *See* de Villiers, *supra* note 4, at 16-17.

15. *Id.* at 16.

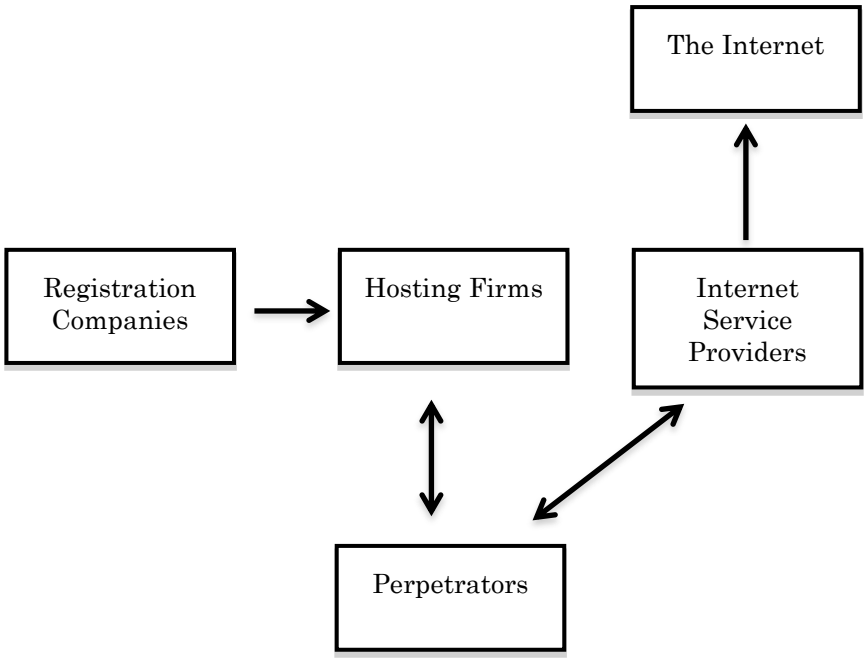
16. A Trojan is a form of malware that discretely convinces users that it is a harmless computer program. *See* Jon Brodkin, *Viruses, Trojans, and Worms, Oh My: The Basics on Malware*, ARS TECHNICA (Feb. 1, 2013, 9:00 AM), http://arstechnica.com/security/2013/02/viruses-trojans-and-worms-oh-my-the-basics-on-malware. The results range from harmless pop-up windows to extensive damage to the operator's computer often providing a gateway to infiltrate the user's computer or network. *Id.* Today, hackers are more likely to be large-scale corporate entities than single perpetrators thereby providing substantial leverage in the online market. *See* John Loveland et al., *Be Afraid, Be Very Afraid: The Rise of Organized Cyber Crime*, CORP. COMPLIANCE & ETHICS INST. (2010), *available at* http://discover.pli.edu/Details/Details?start=0&rows=50&sort=s_title%20asc&fq=~2B~title_id~3A282B22~23683~2229202B~id~3A282B22~23683-CH44~2229~&facet=true&qt=legal_boolean.

17. *See* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 613-15 (E.D. Pa. 2004).

18. *See* INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN), http://www.icann.org/en/resources/registrars (last visited Oct. 25, 2013).

19. *See generally* Braman & Lynch, *supra* note 13, at 249. The ISP industry has seen tremendous growth through the 2000s. *Id.* at 252. This is largely due to diminishing startup costs and the explosive growth of the Internet. *Id.* There are means by which ISPs may be distinguished from one another including geographic region, the services offered, and its fit within the architecture of the Internet including whether it is downstream or upstream, the types of content it packs and whether its services include web hosting. *Id.*

Figure 1



1. The Connection between Malware and Intermediaries

Malware is the most common form of cybercrime and therefore represents the most prevalent means in which cybercriminals interact with intermediaries.[20] Malware has three primary forms.[21] First, a virus reproduces as it spreads across computers deleting and stealing data as it travels.[22] Executable files deliver the virus, which remains dormant until the end user opens the file and triggers the virus.[23] Second,

20. *Cybercrime According to the Experts*, 19 NEXT WAVE 60, 60 (2012), http://www.nsa.gov/research/tnw/tnw192/articles/pdfs/TNW192_article10.pdf.

21. *See* Brodkin, *supra* note 16.

22. *See id. But see* Mann & Belzley, *supra* note 10, at 241 (noting less of a need to hold intermediaries responsible in the area of viruses, spam, phishing, and hacking because of the perceived inability to control the content and because of the market incentive of ISPs to provide a clean network).

23. *See* Brodkin, *supra* note 16. File sharing and email attachments

worms are similar except that they do not rely upon other files, thus, they are often able to spread across vast computer networks.[24] Finally, trojans convince users that they are harmless computer programs.[25] The results range from harmless pop-up windows to extensive damage to the operator's computer.[26] Trojans often provide a means for users to infiltrate the host's computer or network.[27]

Not only does malware attack computers but it also creates "botnets." These are large networks of "zombie" computers that may be harmless to the computer operator but may respond to commands at the cybercriminal's discretion from a controlling server.[28] Criminals who establish botnets frequently rent access to the infected network to other criminals who "monetize" the access.[29] The Russian Business Network (RBN) provides an apt example of a host and the release of a botnet.[30] RBN provides the portal for numerous activities and collects "infrastructure fees" that result from the fraud.[31] In 2007, RBN was responsible for releasing the BOTnet "storm" that controlled between 1 million and 50 million computers.[32] Clients would then pay RBN for unfettered access to a portion of the computers.[33]

---

often spread the virus. *See id.*

24. *See id.*

25. *See id.*

26. *See id.*

27. *See id.* Remote Access Trojans are "beefed up" backdoors that contain a user interface permitting the attacker to issue destructive commands. *See id.* Commentators occasionally refer to malware as a "backdoor" as it bypasses firewalls and executes an object connecting users to the perpetrator's workstation and corresponding network files. *See id.* "Information stealers" often misappropriate information through the use of keystroke recording devices known as "key loggers." *See id.* "Ransomware" on the other hand holds a user hostage until the user compensates the perpetrator to restore the computer. *See id.*

28. *See id.*

29. *See id.*

30. *See* Loveland et al., *supra* note 16.

31. *See id.*

32. *See id.*

33. *See id.*

2. The Regulatory Landscape of the Internet

One symptom of the fact that no one is focusing on the role of intermediaries in cybercrime is that these entities operate in a virtual regulatory no-man's land. The Internet itself is highly decentralized.[34] Its open, virtually lawless architecture was originally designed in a small community that had a high degree of trust.[35] The point was to keep the Internet as free from regulation as possible in order to foster an unfettered exchange of information. At the time, cybercrime was unlikely to be considered a major problem. To the extent that cybercrime was considered a major problem, the assumption was that the marketplace would clear it up through self-regulation.[36]

Although the self-regulatory model above is probably the most closely accurate description of how the Internet actually functions today, three other models suggest that there may be alternative, informal or unofficial, ways to regulate the Internet. These models are: (1) neo-mercantilist; (2) culturalist; and (3) globalism.[37] The neo-mercantilist model suggests that the government intervenes occasionally to police cybercrime to ensure the free flow of commerce within the channels of the Internet.[38] This policing mostly concerns cybercriminals, not intermediaries.

The culturalist model emphasizes the protection offered by the local culture within its regulatory structure.[39] For example, in the United States, although there are no laws specifically designed to hold intermediaries liable for the crimes they

34. *See* CircleID Reporter, *Who Runs the Internet? ICANN Attempts to Clarify the Answer with This Map*, CIRCLEID (Mar. 6, 2013, 9:46 AM), http://www.circleid.com/posts/20130306_who_runs_the_internet_icann_attempts_to_clarify_answer_with_map/. The multiple stakeholders include society, the private sector, governments, research groups, and NGOs. *See id.*

35. *See* Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-Crime*, 29 INT'L J. POLICE STRATEGIES & MGMT. 408, 409, 412 (2006).

36. *See* Kevin A. Meehan, *The Continuing Conundrum of International Internet Jurisdiction*, 31 B.C. INT'L & COMP. L. REV. 345, 353 (2008).

37. *Id.*

38. *See id.* at 354.

39. *See id.*

facilitate, there is a culture wherein prosecutors sometimes make use of a handful of other laws to combat cybercrime. These laws include the Computer Fraud and Abuse Act[40], the CAN-SPAM Act[41], the Electronic Communications, the Privacy Act[42], the Lanham Act[43], and the Racketeer Influence and Corrupt Organizations Act.[44] The necessity of proving *mens rea*, however, renders these laws largely ineffective as applied to intermediaries.[45]

Finally, the globalism model suggests that there is some incipient Internet regulation in the form of international cooperation and agreements such as the Convention on Cybercrime (the Convention).[46] Hardly any of these international agreements discuss host and ISP liability. The Convention merely defines a service provider as "any public or private entity that provides a service via the computer or any entity that stores data for such an online service."[47] The Convention says nothing about imposing liability.[48]

While the neo-mercantilist, culturalist, and globalism models each describe a small part of existing Internet regulation, there is very little regulation as a whole. To the extent that the Internet is regulated at all, its governance is in the hands of a grab-bag of organizations representing divergent stakeholder perspectives.[49] Because many of these stakeholders have different interests, it is questionable whether this multi-stakeholder approach can operate efficiently.[50] Developing countries, for example, argue that they are underrepresented in Internet governance and that an international organization,

40. 18 U.S.C. § 1030 (2012).

41. 15 U.S.C. § 7704 (2012).

42. 18 U.S.C. § 2701.

43. 15 U.S.C. § 1114.

44. 18 U.S.C. § 1962(c)).

45. *See infra* text accompanying notes 107-10 (discussing *mens rea*).

46. *See* Meehan, *supra* note 36, at 355; *see also* Nancy E. Marion, *The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation*, 4 INT'L J. CYBER CRIMINOLOGY 699, 701 (2010).

47. Marion, *supra* note 46, at 705.

48. *See id*. at 705-06.

49. *See* Bevil Wooding, *The Brewing Internet Governance Storm*, CIRCLEID (Aug. 30, 2012, 4:28 PM), http://www.circleid.com/posts/20120830_the_brewing_internet_governance_storm/.

50. *See id*.

such as the International Telecommunications Union (ITU), should expand its regulatory oversight.[51] Most observers would probably agree that the large number of regulatory bodies and lack of any single one with overriding authority has in large part failed to keep the Internet safe. That is why there may be a shift to increasing the international agreements described in the globalism model, as evidenced by the Convention.[52]

Perhaps the most impressive global initiative to regulate the Internet came in 1997, when the forty-seven nations that comprise the Council of Europe commissioned the formation of a comprehensive set of laws to combat cybercrime.[53] The Convention became effective in July 2004 after Lithuania ratified it in March of that year.[54] Twenty-three countries have

51. *See id.* Telecommunications companies are largely dissatisfied with current Internet governance. They feel that they invested in the infrastructure of the Internet and now, compared to the fortunes realized by Google, Skype and Facebook, are being left behind. *See id.*

52. *See infra* notes 53-68 and accompanying text (discussing the Convention). However, this decentralized system enhances governance flexibility and has led to the amazing growth of the Internet. *See* Wooding, *supra* note 49. One centralized entity that governs the Internet is the Internet Corporation for Assigned Names and Numbers (ICANN), which is a private organization that manages IP addresses and domain names. *See* BRIGID GRAUMAN, CYBER-SECURITY: THE VEXED QUESTION OF GLOBAL RULES, AN INDEPENDENT REPORT ON CYBER-PREPAREDNESS AROUND THE WORLD 29 (2012), http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf. The legislative and executive branches of the United States government have cautioned against too much control within a multi-stakeholder Internet governance model. *See* Rebecca MacKinnon, *The United Nations and the Internet: It's Complicated*, FOREIGN POL'Y (Aug. 8, 2012), http://www.foreignpolicy.com/articles/2012/08/08/the_united_nations_and_the_internet_it_s_complicated. However, because cybercrime crosses national boundaries, multilateral efforts are a critical deterrent. John Sinden, Jr., *Cybersecurity at the International Level*, EASTWEST INST. (April 30, 2012), www.ewi.info/cybersecutiry-international-level. The organizations devoted to fighting cybercrime include the International Telecommunication Union (ITU), the Asia-Pacific Economic Cooperation, the European Network and Information Security Agency (ENISA), and the Computer Emergency Response Pre-configuration Team (CERT-EU). *See id.*

53. *See* Marion, *supra* note 46, at 701.

54. *See* LORENZO VALERI ET AL., HANDBOOK OF LEGAL PROCEDURES OF COMPUTER AND NETWORK MISUSE IN EU COUNTRIES 18 n.2 (2006). While the Convention provides a comprehensive framework, its value is largely symbolic and may not be effective otherwise. *See* Marion, *supra* note 46, at 701. One criticism is that even as more countries ratify the Convention, some countries will provide a safe haven for cyber criminals. *See id.* Symbolic legislation does perform the function of "moral educative function" by

since ratified the Convention; the United States Senate did so in 2006.[55] The Convention provided the framework under which signatory countries developed their respective laws to combat cybercrime.[56] The Convention provides three primary offenses: (1) Article 2 governs the illegal accessing of information; (2) Article 5 governs system interference; and (3) Article 4 governs data interference.[57] Intermediary liability, however, is unlikely because of the Convention's demand that all criminal offenses be committed *intentionally*—and intermediaries naturally assert that they are unaware of the criminal activity on their networks.[58]

The laws of each ratifying country had to meet the Convention's minimum threshold. For example, under Article 2 of the Convention,

> [e]ach Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.[59]

Country specific laws must satisfy this provision although

educating people of what is right and wrong behavior. *See id.* at 706. It further provides guidance to those countries considering a regulatory framework. *See id.*

55. *See* Marion, *supra* note 46, at 702.

56. *See* Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 40916.

57. *Id.* at 4-5; *see also* VALERI ET AL., *supra* note 54, at 18. This is just a minimum threshold as countries are free to codify more stringent requirements. *See* Convention on Cybercrime, *supra* note 56, at 4-5.

58. Cedric J. Magnin, The 2001 Council of Europe Convention on Cyber-Crime: An Efficient Tool to Fight Crime in Cyber-Space? 55 (June 2001) (unpublished L.L.M. dissertation, Santa Clara University) (on file with author).

59. Convention on Cybercrime, *supra* note 56, at 4.

some countries have "opted out" of Convention provisions.[60]

The Convention largely mirrors corresponding provisions in the European Council Framework Decision on Attacks against Information Systems (Framework Decision).[61] The Framework Decision provides the baseline for furthering awareness of Cybercrime through the application of meaningful assistance through the cooperation of the judicial system and other domestic authorities.[62] Both the Convention and the Framework Decision share provisions, including those that pertain to aiding and abetting and the liability of legal persons.[63]

At least one commentator has incorrectly asserted that the Convention does not exempt ISPs from criminal liability for the content of third parties based upon the aiding and abetting provision.[64] That suggestion is unfounded, as the Convention is clear that it does not require ISPs to monitor content.[65] Liability would only attach under Article 11 for aiding and abetting if the ISP shared the mental state with the perpetrator.[66] The standard for aiding and abetting "requires the defendant to have (1) substantially assisted another who committed a violation of international law and (2) known that his actions would assist in the illegal or wrongful activity at the time he provided the assistance."[67] Further, Article 12, governing corporate liability, only attaches if an individual with a high degree of authority violates Article 2, 4, or 5 or if a lack of supervision results in an individual perpetrating a crime to benefit the corporation.[68]

60. *See, e.g.*, Treaty Office, List of Declarations Made with Respect to Treaty No. 185, COUNCIL OF EUR., http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1 (last updated Mar. 17, 2014).

61. *See* VALERI ET AL., *supra* note 54, at 18.

62. *See id.*

63. *See id.* at 23. Both the Convention and the Framework Decision require that criminal offences be "punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty." *Id.*

64. *See* Magnin, *supra* note 58, at 63.

65. *See id.* at 64.

66. *See id.*

67. Anne Cheung & Rolf H. Weber, *Internet Governance and the Responsibility of Internet Service Providers*, 26 WIS. INT'L L.J. 403, 470 (2008).

68. *See* Magnin, *supra* note 58, at 65.

B. *Intermediary Liability*

Intermediaries face few repercussions for the activity on their servers and networks, and therefore have little incentive to monitor criminal traffic.[69] The burning question, therefore, is whether regulatory policies should impose indirect liability on intermediaries for activities in which knowledge is difficult to prove.[70] To date, intermediaries such as ISPs have avoided liability despite the fact that they are in a favorable position to monitor and control cybercrime.[71]

In fact, ISPs wield an almost regulatory function online and thereby operate in an environment of control without liability.[72] This regulatory function is bolstered by the

69. *See* NOAH SHACHTMAN, BROOKINGS INST., PIRATES OF THE ISPS: TACTICS FOR TURNING ONLINE CROOKS INTO INTERNATIONAL PARIAHS 3 (2011).

70. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable* 8 (Univ. of Chi. Law Sch., John M. Olin Law & Econ. Working Paper No. 217, 2004) (noting indirect liability arises in those instances in which a party is held liable for the wrongs of another).

71. *See id.* at 4.

72. *See* SHACHTMAN, *supra* note 69, at 3. Ten out of 5,000 ISPs account for around thirty percent of spam worldwide. *See id. But see* BRUCE A. LEHMAN & RONALD H. BROWN, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 116 (1995) ("[I]t is . . . virtually impossible for operators of large systems to contemporaneously review every message transmitted or file uploaded."). ISPs, however, wield power in the amount of information they control and retain. *See* Cheung & Weber, *supra* note 67, at 403-04 (comparing ISPs to "secret police" and "surveillance centers"). In the context of offensive speech, authorities often seek to hold intermediaries such as ISPs liable even absent any knowledge of the content of the speech. *See id.* at 408-09. Therefore, the government has enlisted the services of these intermediaries to monitor the content of the speech even if the intermediary is from a country with different norms concerning protected speech. *See id.* at 409. The result has been an over filtering of legitimate speech in order to capture the intended speech as mandated by the government. *See id.* at 409-10. Not only are ISPs encouraged to censor speech, but they are also policing the Internet by informing governments of suspected content violations. *See id.* at 412. Critics have noted that ISPs perform a regulatory function even though they do not satisfy the "regulatory criterion of being all-encompassing." Braman & Lynch, *supra* note 13, at 253. Further, they do not answer to constituents in a democratic society. *See id.* at 267. For example, ISPs have claimed that they are merely information distributors and not content providers while they have claimed control over the intellectual property they transmit. *See id.*

cooperation between the government and ISPs.[73] For example, the provisions of the Convention mandated communication between ISPs and law enforcement.[74] Further, both Canada and China have relied upon ISPs as informers as well.[75] In the United States, the Court in *American Council on Education v. FCC* held that the 1994 Communications Assistance for Law Enforcement could require ISPs to provide better and more reliable infrastructure to conduct surveillance on behalf of law enforcement.[76] Despite this leverage and power, ISPs rarely self-regulate criminal activity on their networks.[77]

Asserting indirect liability over ISPs is appropriate both because of the better position of ISPs as detectors of nefarious activities and because ISPs are better able to internalize negative externalities.[78] Indirect liability also becomes more attractive when the liable party has an increased ability to influence or prevent "bad" behavior.[79] The vast regulatory control of ISPs illustrates this point.[80] Simple distinctions between ISPs and individual perpetrators further suggest their better position to absorb liability.[81] For example, ISPs tend to maintain a static location and have "deeper pockets" compared to individual perpetrators.[82] In the context of cybercrime, the perpetrators are largely outside the reach of the law.[83] This is true for two reasons. First, the nature of cybercrime conceals the perpetrator and permits the perpetrator to time the attack in order to hide his identity and location.[84] Second, the perpetrators often lack the financial resources to compensate

73. *See* Cheung & Weber, *supra* note 67, at 404.

74. *See* Marion, *supra* note 46, at 704-05.

75. *See* Cheung & Weber, *supra* note 67, at 412-16.

76. Am. Council on Educ. V. FCC, 451 F.3d 226, 233 (D.C. Cir. 2006).

77. *See* SHACHTMAN, *supra* note 69, at 18. For example, the ISP for the notoriously bad host Mc-Colo did not remove Mc-Colo from its network until journalists gathered and presented substantial evidence of its behavior. *See id.*

78. *See* Lichtman & Posner, *supra* note 70, at 22-23.

79. *See id.* at 18.

80. *See id.* at 18-20.

81. *See id.* at 15-16.

82. *See id.* at 15.

83. *See id.*

84. *See id.*

the injured parties.[85] Harmed parties may be too far removed from judgment-proof perpetrators.[86]

Not surprisingly, there are several market-based challenges for ISPs to monitor their networks. ISP profit margins may suffer if they get overly aggressive monitoring online activity.[87] Further, victims may be on a network far removed from the ISP such that the ISP may lack the incentive to police content.[88] Finally, ISPs may only voluntarily absorb the costs of maintaining a clean network when the cost of non-responsiveness is high. For example, a Distributed Denial of Service (DDOS) attack—which results in an expansive overload of traffic on the network—may prompt a swift reaction by ISPs.[89]

One noted problem with instituting a penalty on ISPs for criminal activity on their networks is that a fine or other penalty may discourage ISPs from actively investigating suspicious activity, such as turning a blind eye to the content makes it easier to assert a lack of knowledge.[90] Indirect liability imposed on ISPs may also discourage users from engaging in "self-help" through virus software updates and the maintenance of firewalls.[91] Moreover, further active development of virus software and prophylactic technology

85. *See id.*

86. *See id.* at 15-16, 22-23.

87. *See* SHACHTMAN, *supra* note 69, at 20. There are also economic concerns related to the online marketplace. *See* Lichtman & Posner, *supra* note 70, at 23. Indirect liability will raise the prices to service accounts because of the increased legal liability. *See id.* As a result, select customers may not be able to participate in the market. *See id.* This concern increases when participants within the market prefer the inclusion of customers in the online marketplace. *See id.* The effect of this externality might be limited because the subscriber can often internalize the effect by offering the customer product discounts, and other incentives. *See id.* Cybercriminals, who stand to make significant income from crime are likely to make extensive use of their hosts/ISPs, thus constituting a significant portion of those the ISP's/host's traffic and profits. *See* Kim-Kwang Raymond Choo & Russell G. Smith, *Criminal Exploitation of Online Systems by Organised Crime Groups*, 3 ASIAN J. CRIMINOLOGY 37, 37 (2008).

88. *See* SHACHTMAN, *supra* note 69, at 20.

89. *See id.*

90. *See id.* Alternatively, several have proposed a cleanup fund subsidized by the government and software companies. *See id.*

91. *See* Lichtman & Posner, *supra* note 70, at 26-27.

might also be reduced.[92]

There is a well-developed body of case and statutory law in the United States that shields ISPs from civil liability. Traditionally, those ISPs who facilitate the distribution of communication which could lead to a common law wrong (e.g. defamation) would have been immune from liability, so long as they had no knowledge of the act itself. For example, early on, courts did not hold ISPs liable for the communication of defamatory statements through its equipment if they were a passive distributor compared to a publisher.[93] However, subsequent decisions classified ISPs as publishers whenever they actively manipulated editorial content.[94] This resulted in a reluctance to filter content under the guise that the court would be less likely to view it as a publisher.[95] Subsequently, in *Zeran v. American Online, Inc.*, the Fourth Circuit held that Section 230 of the Communications Decency Act ("CDA") equally immunized both publishers and distributors.[96] Section 230 provides that "[n]o provider or user of an interactive service shall be treated as the publisher or speaker of any information provided by another information content provider."[97] This provision has uniformly shielded ISPs from liability.

Another example of a United States court declining to hold an ISP liable for third party content arose in *Doe v. GTE*

92. *See id.*

93. *See* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 136 (S.D.N.Y. 1991).

94. *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *2 (N.Y. Sup. Ct. May 24, 1995).

95. *See* Lichtman & Posner, *supra* note 70, at 34.

96. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 335 (4th Cir. 1997). Some have argued that the language of Section 230 was interpreted contrary to its plain language. *See* Lichtman & Posner, *supra* note 70, at 36. *But see* Juan Carlos Rodriguez, *Ex-Bengals Cheerleader Scores Win in Internet Defamation Suit*, LAW360 (July 11, 2013, 7:06 PM), http://www.law360.com/articles/456738/ex-bengals-cheerleader-scores-win-in-internet-defamation-suit (reporting recent jury decision attaching liability to the website TheDirty.com for the untrue statements concerning the sex life a Cincinnati Bengals cheerleader in the National Football League). The judge denied protection under the CDA because the website "encouraged development of what is offensive about the content of TheDirty.com website." Rodriquez, *supra* note 96 (internal quotation marks omitted).

97. 47 U.S.C. § 230(c)(1) (2012).

Corp.[98] In *Doe*, college athletes sued GTE Corporation and Genuity Corporation after the two companies used their web hosting services on behalf of several production companies for the sale of the videos of the unclothed athletes in locker rooms.[99] The athletes claimed that the defendants had aided and abetted the production companies in providing web hosting services for activity that violated the Electronic Communications Privacy Act of 1986.[100] The court declined to extend the application of the Act beyond the perpetrators noting that federal courts rarely find secondary liability absent a clear articulation of liability.[101] Further, the court found that defendants were indifferent to the content they hosted and did not intend to promote the wrongdoing of the production companies.[102]

Doe and *Zeran* addressed defamation and privacy concerns, but there was little change in the court's analysis when the court considered ISP liability in the context of malware. An unanswered question after *Zeran* was whether malicious code disseminated by ISPs amounted to information under the CDA. In *Green v. America Online*, Green sued America Online ("AOL") because a hacker sent a program over the AOL network that disrupted Green's computer.[103] The court held that AOL was immune because attaching liability would amount to treating AOL as the publisher of the program.[104] Interestingly, the court disagreed with the plaintiff that the

98. Doe v. GTE Corp., 347 F.3d 655, 655 (7th Cir. 2003).

99. *Id.* at 656.

100. *Id.* at 658. The district court's motion to dismiss relied partly on the CDA, which preempts state or local law but not the Electronic Communications Privacy Act. *See id.* The Electronic Communications Privacy Act provides that

any person who—(a) *intentionally* intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (b) *intentionally* uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication . . . [may face civil liability].

18 U.S.C. § 2511(1) (2012) (emphasis added).

101. *Doe*, 347 F.3d at 658.

102. *Id.* at 659.

103. Green v. Am. Online (AOL), 318 F.3d 465, 469 (3d Cir. 2002).

104. *Id.* at 470-71.

harmful computer program was not "information" under the CDA thereby leaving the liability question perhaps unresolved.[105]

In the United States, the law could treat ISPs as carriers, publishers, or distributors with each classification influencing different levels of potential liability.[106] The carrier classification attaches little liability, as once again, the *mens rea* element is critical.[107] For example, the federal child pornography act has included "knowingly" as the *mens rea* term for each of the offenses pursuant to 18 U.S.C. § 2252.[108] The carrier interpretation is consistent with the laws of both the United Kingdom and Germany.[109] While not entirely clear, Finland, Japan, and Latvia, likely interpret the *mens rea* element in the same manner.[110]

A publisher classification, on the other hand, would attach a high degree of culpability.[111] For example, Sweden appears to apply a strict liability standard on publishers in radio and television for offences related to public order, child pornography, and unauthorized depictions of violence.[112] Finally, a distributor is less likely to face liability compared to a publisher even though the two are difficult to distinguish.[113] Control, is often the cited factor in making the determination, the greater the control of the content the more likely the law is to consider the ISP a publisher.

One apparent shortcoming in the penalty structure applied

105. *Id.* at 471.

106. *See* Mark Tantum, *Internet Crimes: Legal Responsibility of Internet Service Providers*, *in* 14 COMPUTER L. & SEC. REP. 383, 383-86 (1998). Privacy concerns in the postal and telecommunications context limit the analogy because "legislatures have generally adopted the view that postal and communications carriers should only be prosecuted for the carriage of illegal information if they know the nature of the information that they are carrying." *Id.* at 384. ISPs operate in a liability regime that consists of negligence, strict liability, or immunity. *See* Braman & Lynch, *supra* note 13, at 254.

107. *See* Tantum, *supra* note 106, at 384.

108. *See* 18 U.S.C. § 2252 (2012).

109. *See* Tantum, *supra* note 106, at 384.

110. *See id.*

111. *See id.* at 385.

112. *See id.*

113. *See id.*

to intermediaries under United States law is that the remedy is often equitable, thereby providing little disincentive. For example, the Federal Trade Commission (FTC) may seek to shut down "bad" ISPs.[114] The FTC has authority under the Federal Trade Commission Act to prevent unfair and deceptive acts or practices and may seek either injunctive or equitable relief.[115] In 2009, for instance, the FTC shut down Pricewert, an ISP incorporated in Oregon with corporate officials outside of the United States.[116] The FTC argued that "Pricewert [r]ecruits and [w]illingly [d]istributes [i]llegal, [m]alicious and [h]armful [c]ontent" and that it was "fully aware" that it was hosting the content.[117] The FTC further contended that Pricewert was "collud[ing] with its criminal clientele in several areas, including the maintenance and deployment of botnets."[118] Despite these allegations, the FTC merely shut down the ISP. Those damaged by the harmful content never recovered.

More recently, in 2012, Microsoft sued the perpetrators of the Zeus botnets.[119] In connection with the lawsuit, legal officials raided several hosts that were associated the defendants after Microsoft had conducted an extensive investigation.[120] The remedy sought was merely an injunction ordering the isolation of the content and material associated with the botnet.[121] Once again, there was no recovery on behalf of the harmed parties.[122]

Aside from the United States, a handful of countries have

114. *See* Complaint at 1, FTC v. Pricewert LLC, 2009 WL 2749865 (N.D. Cal. June 1, 2009) (No. 509-CV-02407).

115. *See* 15 U.S.C. §§ 5, 45(a), 53(b) (2012).

116. *See* FTC v. Pricewert LLC, No. C-09-2407, 2009 WL 1689598, at *1 (N.D. Cal. June 15, 2009).

117. Complaint at 3, FTC v. Pricewert LLC, 2009 WL 2749865.

118. *Id.* at 4.

119. *See* Motion for Default Judgment and Permanent Injunction, Microsoft Corp. v. Does, No. 12-CV-1335, (E.D.N.Y. Dec. 5, 2012).

120. *See* Jim Finkle, Microsoft Seizes Servers in Zeus Cyberfraud, REUTERS (March 26, 2012, 3:46 PM), *http://www.reuters.com/article/2012/03/26/net-us-cyberfraud-idUSBRE82P0ZD20120326.*.

121. *See* Motion for Default Judgment and Permanent Injunciton, *supra*, note 119.

122. *Id.*.

considered the emerging problem of regulating intermediaries, but little reform has resulted. For example, Nigeria, a country rife with cybercrime, has considered extending regulatory oversight over intermediaries including ISPs.[123] One study in Nigeria found that "[t]here is [a] significant relationship between the awareness of [I]nternet intermediary liabilities and level of misconducts over the Internet in Nigeria."[124] The study further found that ISPs in Nigeria provide little security against cybercrime.[125] Despite these findings, little has changed in Nigeria.[126]

A form of self-regulation, however, appears to have had some effect in Australia. There, the Internet Industry Association developed a voluntary code (icode) in which ISPs identify and inform customers of attacks.[127] More than ninety percent of Australian ISPs have committed to icode.[128] Under icode, if the ISP shows that malware has infected the user's computer, the user is redirected to the icode homepage where self-help tools are available to clean the computer.[129] It is a relatively new program and its effectiveness has yet to bear out.

III. What Can We Learn from Other Countries? Finland v. Lithuania

To explore what can be learned from other countries, the worst-performing country (in terms of "bad" intermediaries), Lithuania, and the best-performing country (in terms of "good" intermediaries), Finland, were selected.[130] The report classifies

123. *See* O.B. Longe et al., *Internet Service Providers and Cybercrime in Nigeria–Balancing Services and ICT Development*, INTERNET GOVERNANCE FORUM SECRETARIAT (2008), http://lawlibraryarchive.contentdm.oclc.org/cdm/ref/collection/p15430coll3/id/146.

124. *Id.* at 9.

125. *See id.* at 9-10.

126. *See id.*

127. ICODE, http://icode.net.au/home-why.php / (last visited Oct. 16, 2013).

128. *See* Hamish Barwick, *IIA Seeks Input into iCode Review from ISPs, Security Vendors*, COMPUTERWORLD (April 3, 2012, 12:15 PM), http://www.computerworld.com.au/article/420418/iia_seeks_input_into_icode_review_from_isps_security_vendors.

129. *See id.*

130. *See* GLOBAL SECURITY REPORT, HOSTEXPLOIT'S WORLDWIDE

hosts, registrars, and ISPs as intermediaries and ranks the corresponding "malicious activity" by country.[131] Lithuania is ranked number one with the highest level of malicious activity of all reported countries, while Finland is ranked number 219 with the lowest level.[132] The United States is ranked number 11.[133]

The gap between high performing Finland and poor performing Lithuania presents an opportunity to examine what factors contribute to the difference.. Do the public laws of Finland or Lithuania account for the difference in country performance? Do cultural factors? What can countries do to become more like Finland and less like Lithuania in terms of intermediary cybercrime?

A. *Legal Environment*

In Lithuania and Finland, law enforcement applies the terms of the Convention as adopted in both countries.[134] In Lithuania, the Ministry of the Interior controls the Police Department.[135] On October 1, 2001, the Lithuanian Criminal Police Bureau established a special Cybercrime Unit that monitors, detects, and prevents violations of the Convention.[136]

Similarly, in Finland, the police enforce the Convention through a dedicated computer crime squad.[137] This national unit resides between the Police Department of the Interior and the local police.[138] Suspected computer related crimes are generally reported to the local police and communicated by the

CYBERCRIME SERIES 4 (2012) (comparing countries' levels of intermediary cybercrime).

131. *See id.* The report concedes that the country of registration for an Autonomous System does not always reflect where the Autonomous System resides. The report includes a secondary measure referencing the physical location of the infrastructure determined from the routing locations. *See id.* at 8.

132. *Id.* at 4.

133. *Id.* at 9.

134. *See* VALERI ET AL., *supra* note 54, at 90, 166-67.

135. *See id.* at 167.

136. *Id.*

137. *See id.* at 98.

138. *See id.*

police to the computer crime squad.[139] Several other reporting mechanisms facilitate the communication of suspected cybercrime in Finland. The Finnish Communications Regulatory Authority includes the Computer Emergency Response Team (CERT-FI) which receives suspected security incidents from telecommunications operators and publishes them online.[140] Further, the Council for Mass Media publishes decisions that are followed by subscribing organizations.[141]

Finland and Lithuania also have similar criminal codes pertaining to cybercrime. Both countries are signatories to the Convention, so the cybercrime laws in each country mirror one another. Table 1 highlights both the provisions in the Convention pertaining to cybercrime and the corresponding laws in Lithuania and Finland.[142] Also included are provisions pertaining to aiding and abetting and corporate liability.[143]

Finland's laws contain more provisions about cybercrime than Lithuania's.[144] However, both countries' cybercrime laws contain similar content. For example, Article 3 of the Convention is encoded in Article 198 of Lithuanian law and three separate provisions in Finnish Law.[145] All of these provisions proscribe the intentional interception of nonpublic computer data,[146] but they only apply to the primary perpetrator; they do not address intermediaries.

B. *Cultural Distinctions*

Differences in Finland, Lithuania, and the United States' laws cannot explain their differing levels of host and ISP cybercrime. In countries where corruption is systemic and endemic, people often lack short-term incentives to change their behavior.[147] So even if a country has codified laws

139. *See id.* at 98-99.
140. *See id.* at 99.
141. *See id.*
142. *See infra* Table 1.
143. *See id.*
144. *See id.*
145. *See id.*
146. *See id.*
147. *See* Anna Persson, Bo Rothstein & Jan Teorell, *Why Anticorruption*

prohibiting corrupt behaviors, those behaviors may persist because corruption is also a function of other key variables such as culture, history, the degree to which and length of time the country has been democratically governed, and the countries' overall level of systemic corruption. It is to these variables that we now turn in explaining the differences between Finland and Lithuania while referencing the United States.

1. Cultural Differences Between Nations

Countries differ in terms of their cultures – their shared values, norms, and attitudes.[148] These differences affect people's propensity to engage in a host of behaviors, including corruption and cybercrime.[149] Geert Hofstede, a pioneer in the study of cultural differences between peoples, proposed a theory of how various dimensions of a nation's culture affect the behaviors of people. [150] Two of these dimensions – power distance and masculinity/femininity – seem to explain differences in host and ISP performance between Finland, Lithuania, and the United States.[151]

Power Distance (PD) measures the degree to which people accept that power is unequally distributed in their culture.[152] The higher a nation's PD score, the more its people accept unequal power distribution and the more comfortable they are with autocracy, paternalism, and top down hierarchy.[153] The more accepting a culture is of PD, the more likely it is to

Reforms Fail–Systemic Corruption as a Collective Action Problem, 26 GOVERNANCE 449 (2013).

148. *See* Geert Hofstede et al., *Measuring Organizational Cultures: A Qualitative and Quantitative Study Across Twenty Cases*, 35 ADMIN. SCI. Q. 286 (1990).

149. *See* Sheheryar Banuri & Catherin Eckel, *Experiments in Culture and Corruption: A Review* 11 (The World Bank Dev. Research Group, Working Paper No. 6064, 2012).

150. *See* Hofstede et al., *supra* note 148, at 286.

151. *See id.* at 288.

152. *See* National Cultural Dimensions, HOFSTEDE CENTRE, http://geert-hofstede.com/national-culture.html (last visited Oct. 16, 2013) [hereinafter HOFSTEDE CENTRE].

153. *See id.*

tolerate unfairness, injustice, and corruption.[154] PD scores appear to correlate with intermediary corruption and cybercrime. For example, Finland, which has a low PD score of 33, and Lithuania, which has a high PD score of 45.[155] The U.S. is in the middle, with a PD score of 40, which also reflects its level of cybercrime between Finland and Lithuania.[156]

Hofstede's masculinity/femininity dimension is also useful in explaining differences between Finland and Lithuania. A masculine society is driven by competition, self-centeredness, and individual success, with success defined by the "winner."[157] A feminine society puts a premium on caring for others.[158] It is a society where one's quality of life signals success, modesty is prized, and standing out from the group is not regarded as admirable.[159] Finland, with a score of 26, is the most feminine society of the three.[160] Lithuania, with a score of 65, is the most masculine.[161] The United States, with a score of 62, is in the middle.[162] This conforms to the expectation that in feminine societies, where people are more concerned about the welfare of others, people are more likely to be outraged by corruption and any situation where one person acts selfishly to the detriment of others, than in masculine societies. In fact, high levels of perceived corruption are correlated with masculinity.[163]

154. *See* James H. Davis & John A. Ruhe, *Perceptions of Country Corruption: Antecedents and Outcomes*, 4 J. BUS. ETHICS 275, 278-79 (2003); Bryan W. Husted, *Wealth, Culture, and Corruption*, 30 J. INT'L BUS. STUD. 339, 343-44 (1999).

155. *See infra* Table 2; *see also* Adura I. Mockaitis, *A Cross-Cultural Study of Leadership Attitudes in Three Baltic Sea Region Countries*, 1 INT'L J. LEADERSHIP STUD. 44, 46 (2005), http://www.regent.edu/acad/global/publications/ijls/new/vol1iss1/mockaitis/cross_cultural.pdf.

156. *See infra* Table 2.

157. *See* HOFSTEDE CENTRE, *supra* note 152.

158. *See id.*

159. *See id.*

160. *See infra* Table 2.

161. *Id.*

162. *Id.*

163. *See* Rajib Sanyal, *Determinants of Bribery in International Business: The Cultural and Economic Factors*, 59 J. BUS. ETHICS 139, 142 (2005); *see also* Husted, *supra* note 154, at 339; Christopher J. Robertson & Andrew Watson, *Corruption and Change: The Impact of Foreign Direct Investment*, 25 STRATEGIC MGMT. J. 385, 389-92 (2004).

2. The Cultural Legacy of Communism Versus Democracy

A legacy of democracy or communism also seems to be a factor in determining a country's level of corruption. Research shows that former communist countries, such as Lithuania, are more vulnerable to corruption than nations that were never communist.[164] Researchers speculate that it is because communist countries had strong "survival" orientations, which have been linked in studies to higher levels of corruption.[165] Studies also support the flip-side: the longer a country's exposure to democracy, the less corrupt it is likely to be.[166]

Lithuania was a communist republic of the former Soviet Union from 1940 until 1990.[167] As with many former communist states, the transition to democracy and a market economy has not overcome the survivalist mentality and culture of corruption.[168] The process of privatization simply created new opportunities for corruption.[169]

Finland and the United States, on the other hand, were never communist or under the Soviet Union. In fact, during the Russian Revolution, Finland defiantly declared independence from Russia, prompting a civil war in which the pro-Bolsheviks were defeated.[170] Finland became a democratic presidential republic in 1919, with its citizens strongly encouraged to own land and participate in the market economy.[171]

The United States, which declared independence in 1776, has been a democracy for the longest of the three countries.

164. *See* Wayne Sandholtz & Rein Taagepera, *Corruption, Culture, and Communism*, 15 INT'L REV. SOC. 109, 110 (2005).

165. *See id.* at 126.

166. *See generally* Daniel Treisman, *The Causes of Corruption: A Cross-National Study*, 76 J. PUB. ECON. 399 (2000).

167. CIA, *Lithuania*, WORLD FACT BOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/lh.html (last visited Oct. 16, 2013).

168. *See* Sandholtz & Taagepera, *supra* note 164, at 109-10.

169. *See id.* at 110.

170. *See* Markus Jäntti et al., *Growth and Equity in Finland* 3-5 (World Inst. for Dev. Econ. Research, Discussion Paper 2006/06), *available at* http://siteresources.worldbank.org/INTWDR2006/Resources/477383-1118673432908/Janti_Saari_and_Vartiainen_Growth_and_Equity_in_Finland.pdf.

171. *Id.*

(Finland didn't give birth to democracy until 1919).[172] Curiously, however, despite the United States being the oldest democracy, it falls between Finland and Lithuania in terms of cybercrime levels.[173]

One possible explanation is that the United States has only been a *full* democracy since 1870, when the Constitution was amended to give African Americans the right to vote with the Fifteenth Amendment.[174] However, this right was not fully realized for many African Americans until the Voting Rights Act in 1965.[175] Women's right to vote in the United States was not added to the Constitution until the 19th Amendment, which was passed in 1920.[176] Finland, in contrast, granted suffrage to all citizens in 1919.[177]

Another possible explanation is that the quality of democracy may be higher in Finland than the United States. Surveys show that Finnish citizens feel that they have more voice in selecting their government, a higher level of freedom of expression and association, and a freer media than American citizens do.[178]

3. Level of Concern About Integrity, Business Climate, Rule of Law, and Judicial Independence

A number of other cultural variables are also useful in explaining differences between the countries. Consider, for

172. *Id.*; CIA, *United States,* WORLD FACT BOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (last visited Oct. 16, 2013).

173. *See* GLOBAL SECURITY REPORT, *supra* note 130, at 9.

174. U.S. CONST. amend. XV.

175. 42 U.S.C. § 1973 (2012).

176. U.S. CONST. amend. XIX; *see also* The Fight for Women's Suffrage (History Channel broadcast 2013), *available at* http://www.history.com/topics/the-fight-for-womens-suffrage.

177. *See* Jäntti et al., *supra* note 170, at 6-9.

178. Finland scores a 1.54; the US a 1.16; and Lithuania a 0.90 on Transparency International's "Voice and Accountability" surveys. *See Voice and Accountability*, TRANSPARENCY INT'L, http://www.transparency.org/country (last visited Sept. 14, 2013). These surveys capture the public's perceptions of the extent to which their country's citizens can participate in choosing their government, expressing themselves freely, associating freely, and how free the media is.

instance, concerns about integrity. Extrapolating from the levels of perceived corruption in the three countries, it is plausible to conclude that a culture of corruption and lack of concern about values is most endemic and widespread in Lithuania and least so in Finland. According to Transparency International, (the premier institution that maps global corruption rates) in 2013 Lithuania rates a low 54 out of 100 in corruption;[179] Finland, a high 90 out of 100; while the US falls in the middle with a 73 out of 100. [180] Transparency International also reports that Lithuania is the worst at controlling corruption, with a score of 0.32; Finland is the best at controlling corruption, with a score of 2.15; while the United States is in the middle, with a 1.23.[181] This correlates precisely with the host and ISP cybercrime rates in these countries.

Other reports and surveys support the conclusion that Lithuania has the most corruption-prone culture, while Finland has the least. The culture of corruption in Lithuania, and its infiltration in the country's upper echelons, for instance, is illuminated in the numerous high-profile cases of government abuse there. Cases involve officers ranging from city mayors, top national minister, upper level officers in the important Ministry of Economy, the Postal Service, the State Social Insurance Fund, and to the speaker of Parliament .[182]

179. *See Corruption Perception Index 2012,* TRANSPARENCY INT'L, http://cpi.transparency.org/cpi2012/results/#myAnchor2 (last visited Nov. 24, 2013).

180. *See infra* Table 4. It is notable that Transparency International rated Finland as the least corrupt country in 2012. *Id.*

181. *See id.* According to Transparency International control of corruption is one of six dimensions of Worldwide Governance Indicators. *Id.*

182. *See BTI 2012: Lithuania Country Report*, BERTELSMANN STIFTUNG, http://www.btiproject.org/fileadmin/Inhalte/reports/2012/pdf/BTI%202012%20Lithuania.pdf (last visited Sept. 14, 2013). Vilius Navickas, the mayor of Vilnius, was forced to resign in 2010 because he had exerted pressure on the auditor of the municipal administration to resign for pursuing investigations about the construction of schools and the effectiveness of central heating in Vilnius. *See id.* at 8. The economic minister failed to declare his private interests in accordance with procedures and has been forced to resign. *See id.* In early 2011, the Prosecutor's General Office charged three high-ranking officials of the Ministry of Economy for a number of corrupt acts. *See id.* High-ranking employees of Lithuania's postal service and state social insurance fund were recently charged with corruption and the abuse of office. *See id.* There was a trial against Viktoras Muntianas, the former speaker of the parliament, who resigned in March 2008 amid allegations that he bribed

Moreover, reports suggest that the number of criminal acts related to corruption are on the rise.[183]

Reports show that Finland, in contrast, is relatively free from the serious, systemic kind of corruption that afflicts Lithuania.[184] The Finnish population takes ethical values, honesty, and legal codes very seriously —that trend that has increased over the past ten years.[185]

Finland's concern with values is reflected in its proactively ethical corporate culture and ethically oriented corporate governance practices, including Internet companies.[186] Finnish corporate governance is characterized by a high degree of self-regulation, resulting in companies often imposing sanctions on one another.[187] Transparency tends to permeate firms, as suggested by the Finnish Limited Liability Companies Act requirement that institutions explain departures from shareholder recommendations.[188] Not surprisingly, Finnish ISPs are known to "self-police" suspicious cybercrime activity, regardless of whether they have a legal obligation to do so.[189] TeliaSonera, a Finnish ISP, for instance, began an automated review system for its network in 1999.[190] It is now fully automated and frequently updated.[191] All this suggests that

a deputy governor of Kaunas County to receive assistance for a relative's business. *See id.*

183. *See id.* The latest available data by the Lithuanian Ministry of Interior shows an increase in the number of criminal acts related to corruption. *See id.* In 2009, 890 such cases were registered, which is up 23% since 2008 (724). *Id.* A total of 479 persons were registered as suspects in corrupt activities, which is 10% more than those registered in 2008 (435). *Id.* It is not known whether this increase is a result of improvements to the fight against corruption or a rise in corrupt activities. *See id.*

184. *See* Ari Salminen, Olli-Pekka Viinamäki & Rinna Ikola-Norrbacka, *The Control of Corruption in Finland*, 9 ADMINISTRATIE SI MGMT. PUB. 81, 81-83 (2007) (Fin.).

185. *See BTI 2012: Lithuania Country Report*, *supra* note 182.

186. *See* DATAMONITOR, COUNTRY ANALYSIS REPORT-FINLAND–IN-DEPTH PESTLE INSIGHTS (2009).

187. *See id.*

188. *See id.*

189. *See* Mirko Zorz, *Behind the Scenes of the Cleanest ISP in the World*, HELP NET SEC. (Apr. 17, 2012), http://www.net-security.org/article.php?id=1703.

190. *See id.*

191. *See id.*

improving the quality of service – rather than merely meeting the minimal threshold of legal obligations—is what drives most ISPs in Finland.[192]

Unlike in Finland, we found no evidence of significant corporate transparency, corporate self-policing or any requirement that institutions explain departures from shareholder recommendations in the Lithuania. Needless to say, there is no evidence of ISPs self-policing in Lithuania.

The United States record on ethical corporate governance is somewhere between Lithuania and Finland. The passage of the Sarbanes-Oxley Act of 2002 improved, corporate transparency.[193] However, corporate transparency is still problematic.[194] In a few, but far from all, industries, American corporations should be commended for self-regulation.[195] United States firms tend not to impose sanctions on each other, as they do in Finland. Nor are United States firms obligated to explain departures from shareholder recommendations.[196] A number of American ISPs have agreed to self-police in certain areas, such as piracy.[197] However, many have not.[198] Corporate governance is a reflection of societal culture and therefore

192. *See id.*

193. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745; *see also* Greg Zegarowski, *Corporate Sustainability After Sarbanes-Oxley Linking Social-Political Initiatives and Small and Medium-Sized Enterprise Resources*, 4 INT'L J. DISCLOSURE & GOVERNANCE 52 (2007).

194. *See, e.g.*, Tessa Hebb, *The Economic Inefficiency of Secrecy: Pension Fund Investors' Corporate Transparency Concerns*, 63 J. BUS. ETHICS 385, 385 (2006).

195. *See* Robert Greenwald, *News Corp: A Study in the Failure of Corporate Self-Regulation*, GUARDIAN (July 26, 2011, 1:00 PM), http://www.theguardian.com/commentisfree/cifamerica/2011/jul/26/news-corporation-joel-klein; *see also* Lisa L. Sharma, Stephen P. Teret & Kelly D. Brownell, *The Food Industry and Self-Regulation: Standards to Promote Success and to Avoid Public Health Failures*, 100 AM. J. PUB. HEALTH 240 (2010).

196. *See* Lucian Arye Bebchuk, *The Case for Increasing Shareholder Power*, 118 HARV. L. REV. 833 (2005); *see also* SEC DIV. OF CORP. FIN., STAFF REPORT: REVIEW OF THE PROXY PROCESS REGARDING THE NOMINATION AND ELECTION OF DIRECTORS (2003), *available at* https://www.sec.gov/news/studies/proxyrpt.htm.

197. *See* Ernesto Van Der Sar, *Has Your ISP Joined the US "Six Strikes" Anti-Piracy Scheme?*, TORRENTFREAK (Aug. 3, 2012), https://torrentfreak.com/isp-six-strikes-anti-piracy-scheme-120803/.

198. *Id.*

different countries manifest different corporate governance practices. Finland is the least corrupt country, Lithuania is the most corrupt and the United States is in between.

There are two other sub-facets of a country's culture that correlate with its overall levels of corruption: level of judicial independence and the degree to which the country has a rule of law.[199] Both of these variables are related to the public trust in government, which correlates with the country's level of integrity.[200] According to Transparency International, in Lithuania, the rule of law is the weakest of all three countries.[201] In Finland, the rule of law is the strongest (one of the strongest in the world) and in the United States the rule of law is in the middle.[202]

According to Transparency International, with a score of 6.4, Finland ranks highest in judicial independence.[203] Lithuania, with a score of 3.4, ranks lowest.[204] The United States is in the middle with a score of 4.9.[205] These results are borne out by other reports that show that in Finland, judges are professionally selected and public trust in the judiciary is

199. *See Judicial Independence,* Transparency Int'l, http://www.transparency.org/country (last visited Sept. 14, 2013). Judicial Independence is an indicator in the Global Competitiveness Index produced by the World Economic Forum. *See generally* WORLD ECONOMIC FORUM, THE GLOBAL COMPETITIVENESS REPORT 12-13 (2013-2014), http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2013-14.pdf. It measures the perceived extent to which the judiciary of the country is independent from influences of members of government, citizens, or firms. *See Judicial Independence*, *supra* note 199. Rule of Law captures perceptions to the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, property rights, the police, and the courts, as well as the likelihood of crime and violence. *See id.* Rule of Law is one of the six dimensions of the Worldwide Governance Indicators. *See id.* Both Judicial Independence and Rule of Law are reported by Transparency International. *See id.*

200. *See* Eric M. Uslaner, *Trust and Corruption*, *in* CORRUPTION AND THE NEW INSTITUTIONAL ECONOMICS (Johann Graf Lambsdorff et al. eds., 2004). Higher levels of public trust yield correlate with lower levels of corruption. *See id.*

201. *See infra* Table 4.

202. *See id*. In Lithuania, there are no or few constraints on the basic functions involved in the separation of powers, especially mutual checks and balances. *See BTI 2012: Lithuania Country Report*, *supra* note 182.

203. *See infra* Table 5.

204. *See id.*

205. *See id.*

high.[206] In Lithuania, judges are not professionally selected and public trust in the judiciary is low;[207] only 20 percent of Lithuanian citizens trust the courts.[208] Therefore, it is these countries' cultural dimensions, more than their laws, that best explain differences in their levels of host and ISP cybercrime.

IV. Recommendations

There are two areas in which recommendations may assist countries such as Lithuania: cultural reforms and legal reforms.

A. *Proposals for Cultural Reform*

Research suggests that it is possible for a people's culture to change and become less vulnerable to corruption.[209] There are examples of cities, such as Hong Kong, which changed from having a culture that accepted corruption as a way of business to one that did not, and of countries whose people became less tolerant of wrongdoing.[210] Many factors are involved in such transformations, some of which stem from the cultural variables outlined earlier.

206. *See How Europeans Trust Courts and Police*, ECON. & SOC. RESEARCH COUNCIL (Feb. 14, 2012), http://www.esrc.ac.uk/news-and-events/features-casestudies/features/19793/how-europeans-trust-courts-and-police.aspx.

207. *See infra* Table 5.

208. *See BTI 2012: Lithuania Country Report*, *supra* note 182 (According to a public opinion poll by Baltijos Tyrimai, only 20% of Lithuania's citizens trust the courts and 71% do not, 19% and 41% respectively in 2008.).

209. *See* Robert Klitgaard, President & Univ. Professor, Claremont Graduate Univ., Speech at the Second Session of the Conference of State Parties to the United Nations Convention Against Anti-Corruption: A Holistic Approach to the Fight Against Corruption (Jan. 29, 2008); *see also* Benny Pollack & Ann Matear, *Dictatorship, Democracy, and Corruption in Chile*, 25 CRIME, L. & SOC. CHANGE 371 (1996).

210. *See* LOCAL INTEGRITY SYSTEMS: WORLD CITIES FIGHTING CORRUPTION AND SAFEGUARDING INTEGRITY (Leo Huberts, Frank Anechiarico & Frédérique Six eds., 2008) (discussing how cities have successfully dealt with corruption); *see also* Alexander E.M. Hess & Michael Sauter, *The Most Corrupt Countries in the World*, USA TODAY (July 14, 2013, 7:02 AM), http://www.usatoday.com/story/money/business/2013/07/14/most-corrupt-countries/2512785/.

1. Enhancing Democratic Institutions

There is a connection between the length of time a country has been a democracy, having a communist legacy, and corruption as discussed above. Given that connection, it would be logical to expect that reforms that enhance democracy would lower corruption in the long term, including cybercrime. There is vast literature on democracy building that outlines how the international community can help build and strengthen democratic institutions and improve a country's level of trust, such as through controlled foreign direct investment and encouraging fiscal transparency and freedom of the press.[211]

2. Civil Society

A key element to stabilizing democracy and enhancing trust between people in a country involves supporting its civil society, the sphere of non-government organizations in which citizens voluntarily associate to share and advance common interests.[212] These organizations generally include voluntary associations and non-profits organizations such as religious institutions, clubs, social movements, networks, and other

211. *See* PETER BURNELL, BUILDING BETTER DEMOCRACIES: WHY POLITICAL PARTIES MATTER (2004), http://www.wfd.org/upload/docs/WFDBBD5_noprice.pdf; *see also* John C. Bertot, Paul T. Jaeger & Justin M. Grimes, *Using ICTs to Create a Culture of Transparency: E-government and Social Media as Openness and Anti-Corruption Tools for Societies*, 27 GOV'T INFO. Q. 264 (2010); Ivar Kolstad & Arne Wiig, *Is Transparency the Key to Reducing Corruption in Resource-Rich Countries?*, 37 WORLD DEV. 521 (2009); Lorenzo Pellegrini & Reyer Gerlagh, *Causes of Corruption: A Survey of Cross-Country Analyses and Extended Results*, 9 ECON. GOVERNANCE 245 (2008) (discussing the importance of newspapers to lower corruption levels); Robertson & Watson, *supra* note 163, at 385.

212. *See* Pellegrini & Gerlagh, *supra* note 211, at 245 (finding that medium-long exposure to uninterrupted democracy is associated with lower corruption levels); *see also* Axel Hadenius & Fredrik Uggla, *Making Civil Society Work, Promoting Democratic Development: What Can States and Donors Do?*, 24 WORLD DEV. 1621 (1996) (discussing the importance of a vigorous civil society for democratic stability and performance); Vilmos F. Misangy, Gary R. Weaver & Heather Elms, *Ending Corruption: The Interplay Among Institutional Logics, Resources, and Institutional Entrepreneurs,* 33 ACAD. MGMT. REV. 750 (2008).

informal groups.[213] It is through these organizations that people exercise the freedom to come together and give voice to their individual and collective wishes, dreams, and expectations, share their interests, express their values and preferences, and build trust in each other.[214] This kind of civic engagement can help fight corruption.[215] Reform initiatives should thus support countries' civil society organizations to strengthen the underlying civic participatory infrastructure – the vehicle through which trust can grow and democracies develop.[216]

3. Judicial Independence and the Rule of Law

Reformers should also design methods to strengthen judicial independence and the rule of law – two indicators of a country's democratic vitality,[217] the level of public trust in its courts and justice system, and its overall corruption levels.[218] There is a great deal of literature on how to build and bolster these institutions. [219]

4. Power Distance

We might expect that, as democratic institutions develop, people would be increasingly less comfortable with power being

213. *Non-Governmental Organizations*, UNITED NATIONS RULE OF LAW, http://www.unrol.org/article.aspx?article_id=23 (last visited Sept. 13, 2013)

214. *See* Nicholas Babchuk & John N. Edwards, *Voluntary Associations and the Integration Hypothesis*, 35 SOC. INQUIRY 149 (1965).

215. *See* Frank Anechiarico, *Administrative Culture and Civil Society: A Comparative Perspective*, 30 ADMIN. & SOC'Y 13 (1998).

216. *See* UNITED NATIONS ECON. & SOC. COMM'N FOR W. ASIA, ENHANCING CIVIL SOCIETY PARTICIPATION IN PUBLIC POLICY PROCESSES (2005), http://www.escwa.un.org/information/publications/edit/upload/sdd-10-tp1.pdf.

217. *See* Hon. John M. Walker, Jr. & Daniel J.T. Schuker, *Strengthening Judicial Independence in the New Constitutional Democracies of Central and Eastern Europe*, 37 YALE J. INT'L L. 43 (2012).

218. *See* Daniel Lederman, Norman V. Loayza, & Rodrigo R. Soares, *Accountability and Corruption: Political Institutions Matter*, 17 ECON. & POL. 1, 1 (2005).

219. *See e.g.*, PIPPA NORRIS, DRIVING DEMOCRACY: DO POWER-SHARING INSTITUTIONS WORK? (2008); Stefan Wolff, *Building Democratic States After Conflict: Institutional Design Revisited*, 12 INT'L STUD.ZZ REV. 128 (2010).

unequally distributed. If so, the country's PD would decline, which is associated with lower levels of corruption. This effect might be achieved through educational initiatives that teach students about the value of democracy and equality of opportunity.

5. Masculinity/femininity

As discussed earlier, the more feminine the culture, the less corrupt. The traditional understanding is that the number and quality of institutions that engage in caring for others in a society is an expression of the people's level of empathy and compassion in that society.[220] However, the logic set forth by scholars Shadnam and Thomas—that integrity flows, not only from communities of individuals to organizations, but also from organizations back to communities of individuals—suggests that if reformers increase the number and quality of empathic institutions in a society, that could make its people more caring in the long-run too. [221] If so, reformers should not neglect interventions that create institutions that serve others with compassion in a country.

6. Law Enforcement

Lastly, improving the policing of corruption and cybercrime and enhancing the penalties for those who engage in wrongdoing can change a culture of corruption.[222] Enhancing law enforcement can change a culture, not only through deterrence, but also by signaling that society strongly values

220. *See* Kees van den Bos et al., *The Psychology of Voice and Performance Capabilities in Masculine and Feminine Cultures and Contexts*, 99 J. PERSONALITY & SOC. PSYCHOL. 638, 639 (2010); Warren French & Alexander Weis, *An Ethics of Care or an Ethics of Justice*, 27 J. BUS. ETHICS 125, 126-27 (2000).

221. *See* Masoud Shadnam & Thomas B. Lawrence, *Understanding Widespread Misconduct in Organizations: An Institutional Theory of Moral Collapse*, 21 BUS. ETHICS Q. 379, 381 (2011).

222. *See* Catherine D. Marcum, George E. Higgins & Richard Tewksbury, *Doing Time for Cyber Crime: An Examination of the Correlates of Sentence Length in the United States*, 5 INT'L J. CYBER CRIMINOLOGY 825, 833 (2011).

honest and integrity.[223] While there will always be scofflaws, it is the predominant signals that society consistently and repeatedly sends that affect the culture most.[224] Being serious about prosecuting wrongdoing is one of the key ways to demonstrate this.

B. *Proposal for Legal Reform*

Changing a society's culture, however, takes time.[225] So until a cultural shift occurs, legal reform that deals with the short-term is in order. Imposing liability on intermediaries is a key strategy for improvement. While this recommendation would apply to individual countries, collectively they would have a global impact.[226]

The recommended liability scheme modeled below consists of several layers of coordination between the government and those who have been victimized by cybercrime.[227] First, a regulatory body, such as the Cybercrime Unit within the Lithuanian Criminal Police Bureau, could publish an updated list of most nefarious hosts, those most closely aligned with cybercriminals.[228] The hosts would then have the opportunity

223. *See generally* ERNEST VAN DEN HAAG, PUNISHING CRIMINALS: CONCERNING A VERY OLD AND PAINFUL QUESTION 3-7 (1975).

224. *See* LYDIA G. SEGAL, BATTLING CORRUPTION IN AMERICA'S PUBLIC SCHOOLS (2004); *see generally* Raymond Fisman & Edward Miguel, *Corruption, Norms, and Legal Enforcement: Evidence from Diplomatic Parking Tickets*, 115 J. POL. ECON. 1020 (2007); Petter Langseth, *Prevention: An Effective Tool to Reduce Corruption*, GLOBAL PROGRAM AGAINST CORRUPTION CONF. (1999), http://www.unodc.org/pdf/crime/gpacpublications/cicp2.pdf; Marie Talec, *Comparative Law: Of the Impact of Legal Systems on Corruption – A Comparative Study of France and Finland*, ACADEMIA.EDU 15, http://www.academia.edu/835544/Of_the_impact_of_legal_systems_on_corruption_-_Comparative_study_of_France_and_Finland (last visited Oct. 18, 2013).

225. *See* DANIEL CHIROT, HOW SOCIETIES CHANGE (SAGE Publications 2011).

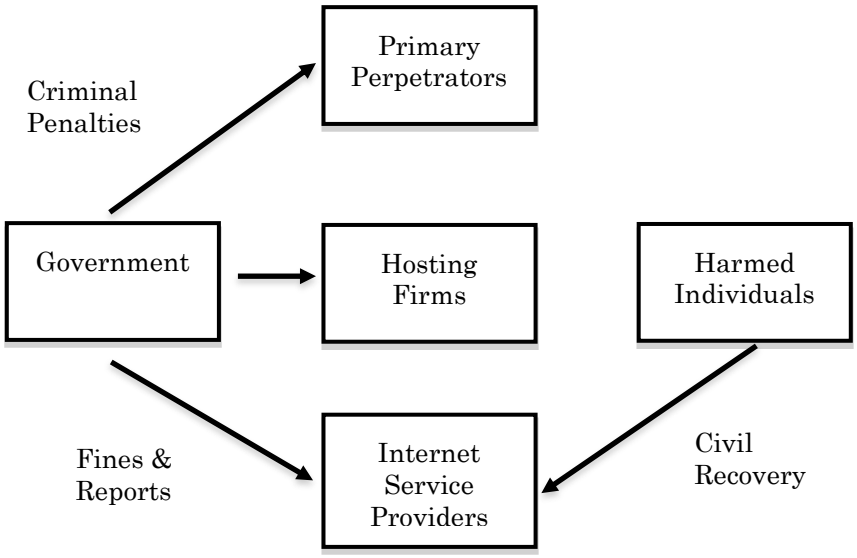
226. *See* Lichtman & Posner, *supra* note 70, at 30; *see also* Tomer Broude & Doron Teichman, *Outsourcing and Insourcing Crime: The Political Economy of Globalized Criminal Activity*, 62 VAND. L. REV. 795, 826-27 (2009).

227. *See* Broadhurst, *supra* note 35, at 416 (noting the need for cooperation between law enforcement and private citizens).

228. *See* SHACHTMAN, *supra* note 69, at 24. Regulators could apply the

to remove themselves from the list within a specified period through remedial action.[229] Those remaining on the list would be subject to governmental fines.[230] Next, the affiliated ISP could be subjected to both regulatory fines imposed by the government and independent private rights of action by victims of cybercrime on the ISPs network if it does not discontinue its relationship with the host.[231] Figure 2 represents a schematic of the liability scheme.

Figure 2



There are a number of benefits to this model. First, it imposes liability on the static and well-funded ISP that also plays the part of a pseudo online regulator.[232] As noted above, absent liability on behalf of ISPs harmed parties are often left

methodology in the Host Exploit reports for instance. *See* GLOBAL SECURITY REPORT, *supra* note 130.

229. *See* SHACHTMAN, *supra* note 69, at 24.

230. *See id.*

231. *See id.*

232. *See supra* text accompanying notes 70-86.

without a remedy as they hunt individual perpetrators and underfunded hosts.[233] Further, it removes the hurdle of imposing a knowledge element on behalf of ISPs. ISPs would, therefore, have a legal duty to monitor the list of "bad" hosts.[234]

Second, the scheme incorporates the culpability of hosts.[235] The host would be front and center on published reports and subjected to fines.[236] Admittedly, locating and tracking shifty hosts will present a challenge to regulatory bodies and the fines may only have a minor effect.[237] However, it is the relationship with the ISPs that will create the greatest deterrent as hosts remaining on the list will be unable to find ISPs willing to work with them.[238]

Third, an important component of the scheme is that it limits the government's involvement by relying on private parties to initiate lawsuits against ISPs. Norms are formed on networks and those norms are enforced in *several* manners.[239] It may take its form in public enforcement with not only criminal liability but also tort liability.[240] Thus, not only do domestic criminal codes and international agreements play a role in deterring cybercrime so too does private law.[241] There is an inherent lack of incentive structure in public law schemes

233. *See id.*

234. *See id.*

235. *See id.* (discussing quasi regulatory function of ISPs); *see also* SHACHTMAN, *supra* note 69, at 23 (noting criticism of the scheme that ignores culpability of hosts).

236. *See* SHACHTMAN, *supra* note 69, at 23

237. *See id.*

238. *See generally* SHACHTMAN, *supra* note 69, at 23.

239. *See* Amitai Aviram, *Network Responses to Network Threats: The Evolution into Private Cybersecurity Associations*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 143,143 (Mark F. Grady & Francesco Parisi eds., 2006).

240. *See id.* at 145. Alternatively, norms may be enforced through private legal systems which arise when norms are enforced by non-governmental institutions. *See id.* For example, parties could enter into a private contract that would thereby assign rights privately but would rely upon the court systems to enforce those rights. *See id.*

241. *See* Broadhurst, *supra* note 35, at 412. "[T]he role of public-private police partnerships in the market-place and the emergence of civil society on the Internet combined with public awareness has become essential to contain cyber-crime amongst ordinary users." *Id.* at 413. The Convention contemplates a framework of cooperation between "private police" and NGOs to successfully fill the gaps within the sovereign state system. *See id.* at 414.

because it often inserts uninformed government officials into the economy.[242] Further, governments often decline to pursue the hackers because of either a lack of resources or because the state is providing some support for its activities.[243] This is particularly true in countries such as Lithuania where corruption is more prevalent.[244] Furthermore, to the extent that intermediaries are being shut down now, it is often the result of investigations by the private community.[245] Here, harmed parties have direct recourse against ISPs.

V. Conclusion

Fighting cybercrime has proven to be a daunting task. This Article highlights new avenues to tackle the problem by focusing on how hosts and ISPs can be corralled into the fight against cybercrime. The Article proposes legal reforms that impose liability in a manner designed to have an effective impact while preventing ISPs or hosts from going out of business. It also proposes societal reforms to shift the culture and business environment to be less tolerant of corruption and more ethically proactive. These reform initiatives will require a great deal of effort and commitment from members of the international community in addition to domestic efforts. However difficult, these reforms and efforts are essential to securing a safe and reliable Internet.

242. *See* Juan Javier del Granado, *The Genius of Roman Law From a Law and Economics Perspective*, 13 SAN DIEGO INT'L L.J. 301, 302 (2011) ("Private law as a system of incentives and a means of communication allows people with information to make decisions and people with incentives to take action in the economy.").

243. *See* Loveland et al., *supra* note 16.

244. *See* Gary S. Becker & George J. Stigler, *Law Enforcement, Malfeasance, and Compensation of Enforcers*, 3 J. LEGAL STUD. 1, 2-3 (1974) (contending that there would be less incentive to bribe thereby diminishing the deterrent effect if private enforcers were compensated via the phones collected from offenders).

245. *See supra* text accompanying note 77.

Table 1—Convention Provisions[246]

	Convention	Lithuania Laws	Finland Laws
Article 2 – Illegal Access	[Each party country shall adopt domestic laws] when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	Article 198 Misappropriation and Dissemination of Computer Information Article 198-1 Illegal Access to Computer or to Network	Penal Code, Chapter 38, Section 8 (Computer break-in)
Article 3 – Illegal Interception	[Each party country shall adopt domestic laws] when committed intentionally, the	Article 198 Misappropriation and Dissemination of Computer Information	Penal Code, Chapter 38, Section 3 (message interference) Penal Code,

246. *See generally Cybercrime Legislation Country Profile: Finland*, COUNCIL OF EUR. (Feb. 2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Finland_2009_February.pdf; *Cybercrime Legislation Country Profile: Lithuania*, COUNCIL OF EUR. (May 30, 2007), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Lithuania_2007_May.pdf.

	interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.		Chapter 38, Section 4 (aggravated message interference) Penal Code, Chapter 38, Section 8, paragraph 2
Article 4 – Data Interference	[Each party country shall adopt domestic laws] when Committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.	Article 196 Destruction or Change of Computer Information	Penal Code, Chapter 35, Section 1 (criminal damage)
Article 5 – System Interference	[Each party country shall adopt domestic laws] the serious hindering without right of the	Article 197 Destruction or Replacement of Software, Disruption of the Operation of	Penal Code, Chapter 38, Section 5 (interference) Penal Code, Chapter 38,

	functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	Computer Network, Data bank or Information System	Section 7a (interference in computer system) Penal Code, Chapter 38, Section 7b (aggravated interference in computer system)
Article 11 – Attempt and aiding and abetting	[Each party country shall adopt domestic laws] aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.	Article 25 Conspiracy and Forms of Conspiracy	Penal Code, Chapter 5, Section 5 (instigation) Penal Code, Chapter 5, Section 6 (abetting)
Article 12 – Corporate Liability	1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by	Article 22 Criminal Liability of Enterprises	Penal Code, Chapter 9, Section 1 (scope of application) Penal Code, Chapter 9, Section 2 (prerequisites for liability) Penal Code, Chapter 9, Section 3 (connection offender and

	any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a. power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention		corporation)

	for the benefit of that legal person by a natural person acting under its authority.		

Table 2[247]

	United States	Finland	Lithuania
Power Distance	The US scores a 40. Within American organizations, hierarchy is established for convenience, superiors are always accessible and managers rely on individual employees and teams for their expertise. Both managers and employees expect to be consulted and information is shared frequently. At the same time, communication is informal, direct and participative.	Finland scores a 33 which means that the following characterizes the Finnish style: Being independent, hierarchy for convenience only, equal rights, superiors accessible, coaching leader, management facilitates and empowers. Power is decentralized and managers count on the experience of their team members. Employees expect to be consulted. Control is disliked and attitude towards managers are informal and on first name basis. Communication is direct and participative.	45

247. Finland, HOFSTEDE CENTRE, http://geert-hofstede.com/finland.html (last visited Nov. 24, 2013).

Individualism	The US scores a 91. The expectation is that people look after themselves and their immediate families. There is also a high degree of geographical mobility in the United States and most Americans are accustomed to doing business with, or interacting, with strangers. In the business world, employees are expected to be self-reliant and display initiative.	Finland scores a 63. Individuals are expected to take care of themselves and their immediate families only. In individualistic societies offence causes guilt and a loss of self-esteem, the employer/employee relationship is a contract based on mutual advantage, hiring and promotion decisions are supposed to be based on merit only, management is the management of individuals.	50
Masculinity / Femininity	The US scores a 62. It is considered a "masculine" society. Behavior in school, work, and play are based on the shared values that people should "strive to be the best they can be" and that "the winner takes all". Typically, Americans "live to work" so that	Finland scores a 26. It is considered a feminine society. The focus is on "working in order to live", managers strive for consensus, people value equality, solidarity and quality in their working lives. Conflicts are resolved by compromise and negotiation. Incentives such as free time and flexibility are	65

	they can earn monetary rewards and attain higher status based on how good one can be. Conflicts are resolved at the individual level and the goal is to win.	favored. Focus is on well-being, status is not shown.	

Table 3—Corruption[248]

	United States	Finland	Lithuania
Corruption Perception Index	2012: Rank: 19 /176 Score: 73 /100	2012: Rank: 1 /176 Score: 90 /100	2012: Rank: 48 /176 Score: 54 /100
Control of Corruption	2010: Percentile Rank: 86% Score: 1.232890271	2010: Percentile Rank: 98% Score: 2.14583654	2010: Percentile Rank: 66% Score: 0.322105477

Table 4—Rule of Law

	United States	Finland	Lithuania
Rule of Law	2010: Percentile Rank: 91% Score: 1.584584729	2010: Percentile Rank: 100% Score: 1.971099617	2010: Percentile Rank:72% Score: 0.760096151

248. *Corruption by Country, TRANSPARENCY INT'L, http://www.transparency.org/ (last visited Nov. 24, 2013).*

Table 5—Judicial Independence[249]

	United States	Finland	Lithuania
Judicial Independence	2011-2012 Rank: 36 /142 Score: 4.9 /7	2011-2012 Rank: 4 /142 Score: 6.4 /7	2011-2012 Rank: 84 /142 Score: 3.4 /7

249. *Id.*