Science and Technology Law Review

Volume 15 | Number 3 Article 3

2012

The Offline Defense of the Internet: An Examination of the Electronic Frontier Foundation

Johnny Nhan

Bruce A. Carroll

The Offline Defense of the Internet: An Examination of the Electronic Frontier Foundation

*Johnny Nhan**
*Bruce A. Carroll***

The growing regulation and commercialization of the Internet has threatened to erode and undermine its core cultural principles of freedom and autonomy. This has triggered many individuals and organizations to defend Internet culture. This project analyzes the institutional design and culture of the Electronic Frontier Foundation ("EFF") within the context of Internet culture. We analyze significant EFF cases as primary-party supporter and amicus curiae to compare and contrast the role of one of the leading defenders of free speech, Internet security, privacy, innovation, and consumer rights manifested through a policy of freedom and autonomy on the Internet. Specific litigation strategies, public policy, and extra legal factors are considered in order to qualitatively and quantitatively examine the EFF's role in the development and protection of Internet culture.

The Internet is considered by many to be a distinct space insulated from the rules of the physical world and governed by a separate set of norms.[1] The Internet has collectively rejected attempts to apply rules and regulations that govern the physical world, and perceives such attempts at applying social control as threats against the sovereignty of the space.[2] John Perry Barlow declared the independence of cyberspace, which underscored the egalitarian and non-hierarchical nature of the Internet.[3] The declaration specifies that cyberspace is organic and does not conform to rules that govern territory defined in the physical world.[4] Instead, cyberspace is "a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth . . . a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being co-

---

* Dr. Carroll is an Assistant Professor in the Department of Criminal Justice at Texas Christian University.

** Dr. Nhan is an Assistant Professor in the Department of Criminal Justice at Texas Christian University.

1. *See* LAWRENCE LESSIG, CODE: VERSION 2.0, at 3 (2006), *available at* http://codev2.cc/dowload®emix/Lessig-Codev2.pdf; David R. Johnson & David Post, Symposium, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996).

2. *See, e.g.*, LESSIG, *supra* note 1, at 3; Johnson, *supra* note 1, at 1379; John Perry Barlow, *A Declaration of the Independence of Cyberspace*, EFF.ORG (Feb. 8, 1996), https://www.projects.eff.org/~barlow/Declaration-Final.html.

3. Barlow, *supra* note 2.

4. *Id.*

erced into silence or conformity," where "legal concepts of property, expression, identity, movement, and context do not apply."[5]

Despite being declared a sovereign, self-governing virtual territory comprised entirely of disembodied thoughts and ideas, the Internet has increasingly been used as a tool for terrorism, crime, and other illegal acts warranting official forms of social control. Such acts draw the attention of lawmakers and other official entities seeking to apply rules and laws to govern the space. For instance, Congress recently proposed H.R. 3523, known as the Cyber Intelligence Sharing and Protection Act ("CISPA"), which is designed to secure government and private information network systems against degradation, disruption, and destruction by "cyber threats."[6] The proposed bill has been criticized for its vague descriptions of cyber threats and targets that include all government and private intellectual property—essentially giving the government power to circumvent Fourth Amendment privacy protections under the auspices of national security.[7] One cyber-security expert quotes a Mozilla representative as stating, "CISPA has a broad and alarming reach that goes far beyond Internet security. The bill infringes on our privacy, includes vague definitions of cybersecurity, and grants immunities to companies and government that are too broad around information misuse."[8]

The attempts at controlling the Internet have fueled adamant offline defense. Founded in 1990, the Electronic Frontier Foundation ("EFF") is a digital rights advocacy group consisting of lawyers, policy analysts, activists, and technologists that considers itself the Internet's "first line of defense" against actions that attempt to limit or control the sovereign nature of cyberspace.[9] Ironically, the group must protect free speech, privacy, innovation, and consumer rights, all of which it considers under attack by legislation in the offline legal arena despite considering cyberspace a completely separate space.[10]

This paper examines the EFF's choices in both the legal strategies employed and nature of cases undertaken to determine legal and extra-legal variables that may influence judicial decisions. First, we review the literature

5. *Id.*

6. Cyber Intelligence Sharing and Protection Act ("CISPA"), H.R.3523, 112th Cong. (2011).

7. *See* Andy Greenberg, *Mozilla Slams CISPA, Breaking Silicon Valley's Silence on Cybersecurity Bill*, FORBES (May 1, 2012, 8:01 PM), http://www.forbes.com/sites/andygreenberg/2012/05/01/mozilla-slams-cispa-breaking-silicon-valleys-silence-on-cybersecurity-bill/.

8. *Id.*

9. ELEC. FRONTIER FOUND., *About EFF*, EFF.ORG, https://www.eff.org/about (last visited Oct. 8, 2012).

10. *Id.*

on the application of law and legal rights on the Internet.[11] Next, we discuss the methods of inquiry.[12] Patterns extracted from coded case types, nature of cases, and coded other variables reveals the EFF's legal strategies and attitudes towards applying and protecting online freedom.[13] Finally, we offer some concluding thoughts and future research directions.[14]

I. REVIEW OF THE LITERATURE

A. The Emergence of Internet Rights Advocacy

The application of online legal protections originates, in large part, from a history of conflict between government agencies, private industry, and general Internet users.[15] This conflict stems from the divergent activities of each group that may be considered violations of the law.[16] These activities range from unauthorized file sharing to surveillance. However since it takes place online, the activities lie within an unresolved gray area of the law. Three primary areas will be discussed: Internet piracy, intelligence gathering, and the nature of EFF cases.

B. Internet Piracy

In the 1990s, the increase in digital music was coupled with an avenue of widespread distribution. The Motion Picture Experts Group ("MPEG") developed and released a standard codex for digital music compression in 1996, which allowed large audio files to be more easily stored and digitally transferred online through slower dial-up modems.[17] The Audio Layer 3 (MPEG-1 Layer-3 or "MP3") digital music compression open format became an industry standard and ultimately ubiquitous with several technological advances.[18] A landmark court ruling in 1999 against the music industry determined that digital media devices did not violate copyright law, leading the way to a "digital music revolution."[19] Concurrently, websites like MP3.com

11. *See infra* Part I.A.

12. *See infra* Part I.B–D.

13. *See infra* Part II.

14. *See infra* Part III.

15. *See generally* ELEC. FRONTIER FOUND., *A History of Protecting Freedom Where Law and Technology Collide*, EFF.ORG, https://www.eff.org/about/history.

16. *See generally id.*

17. KARLHEINZ BRANDENBURG, FRAUNHOFER INST. FOR INTEGRATED CIRCUITS FHG-IIS A, MP3 AND ACC EXPLAINED at 1 (1999) (Ger.), *available at* http://telos-systems.com/techtalk/hosted/Brandenburg_mp3_aac.pdf.

18. *See id.* at 2.

19. Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1073, 1081 (9th Cir. 1999).

were evolving[20] into peer-to-peer file sharing services, such as Napster, and began freely distributing entire albums online.[21] Finally, the development and rapid adoption of high-speed broadband Internet connections significantly increased the speed and volume of unauthorized music distribution.[22]

The widespread online distribution of music drew the attention of Hollywood, initially focusing on the distribution and sale of counterfeit products.[23] During the early 2000s, the music and movie industry, represented by the Recording Industry Association of America ("RIAA") and the Motion Picture Association of America ("MPAA") respectively, were aggressively targeting optical media pirates.[24] For example, the RIAA confiscated 338,458 counterfeit CDs in 1998 and shut down three factories in California.[25]

By 2000, Hollywood recognized the threat posed by Napster and other online file sharing services and began taking legal action.[26] The first lawsuit was filed by A&M Records, representing the rock band Metallica, suing Napster for making a single freely available to the public before its official

20. Andrew Burke & Chris Montgomery, *You Say You Want a Revolution?: A Case Study of MP3.com*, 1 INT'L J. ENTREPRENEURSHIP EDUC., no. 1, 2002, at 107.

21. KEVIN ALVES & KATINA MICHAEL, UNIVERSITY OF WOLLONGONG FACULTY OF INFORMATICS, THE RISE AND FALL OF DIGITAL MUSIC DISTRIBUTION SERVICES: A CROSS-CASE COMPARISON OF MP3.COM, NAPSTER AND KAZAA (2005) (Austl.), *available at* http://www.ro.uwo.au/infopapers/379.

22. *Id.* at 2–3.

23. IFPI, GOOD BUSINESS PRACTICES FOR OPTICAL DISC MASTERING & MANUFACTURING PLANTS at 2, *available at* http://www.ifpi.org/content/library/good_business_practices.pdf (last visited Oct. 8, 2012).

24. *See, e.g.*, David Kravets, *File Sharing Lawsuits at a Crossroads, After 5 Years of RIAA Litigation*, WIRED.COM (Sept. 4, 2008, 2:55 PM), http://www.wired.com/threatleavel/2008/09/proving-file-sh/; David Kravets, *MPAA Helped Cops Nab Hundreds of Movie Pirates*, WIRED.COM (Aug. 18, 2008, 3:52 PM), http://www.wired.com/threatlevel/2008/08/mpaa-helped-for.

25. RECORDING INDUS. ASS'N OF AM., *RIAA Releases Yearend Anti-Piracy Statistics: CD and Internet Piracy Take Center Stage*, RIAA.COM (Apr. 6, 2999), http://www.riaa.com/news/item.php?news_year_filter=1999&resultpage=9&id=89A95D73-257D-1CA0-3C67-623FAFBE54EF.

26. *See, e.g.*, Janelle Brown, *MP3 Free-For-All*, SALON.COM (Feb. 3, 2000, 11:00 AM), http://www.salon.com/2000/02/03/napster/; Brad King, *Bracing for the Digital Crackdown*, WIRED.COM (Aug. 22, 2202), http://www.wired.com/politics/law/news/2002/08/56481?currentPage=all.

release date.[27] They argued that the free release adversely affected Metallica's potential CD music sales.[28]

This lawsuit highlighted complex legal issues focused on the similarities and differences between activities in "real life" and in the online environment. First, Napster argued that it was merely a file indexing service, which meant that it functioned only to broker transactions between individual users (peers) without regard to the actual content distributed.[29] Therefore, it argued, it was not directly responsible for copyrighted content.[30] Second, it brought up an argument challenging the legal notion of possession.[31] Jonathan Sterne explains that since MP3 files are considered products "without commodity form" and do not require much labor to produce, which is often used to justify the perception of the files as substantively different from physical mediums for music.[32] Digital forms of property that reside online are not equivalent to their real-life counterparts.[33] However, Hollywood began aggressively applying legal rules to the online environment.

Hollywood lobbyists advocated for key Internet copyright legislation and suing individual users for copyright infringement. In the late 1990s, the No Electronic Theft Act[34] and the "Sonny Bono Act,"[35] increased penalties for copyright violations while extending the copyright period, respectively. This was coupled with the Digital Millennium Copyright Act ("DMCA"), which addressed the circumvention of copyright protection technologies.[36] These legislative changes gave Hollywood robust legal tools to fight online piracy. Consequently, from 2003 to 2008, the RIAA shifted its strategy from

27. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1013 (9th Cir. 2001) (reviewing on appeal the grant of a preliminary injunction by a Northern District of California court); *see also* Metallica v. Napster, Inc., C 00-4068 MHP, MDL C 00-1369 MHP, C 00-3997 MHP, 2001 WL 777005 (N.D. Cal. Mar. 5, 2001) (order issued in accordance with the Ninth Circuit's decision in *A&M Records*).

28. *A&M Records*, 239 F.3d at 1016–17.

29. *Id.* at 1024.

30. *Id.* at 1024.

31. *Id.* at 1014.

32. Johnathan Sterne, *The MP3 as Cultural Artifact*, 8 NEW MEDIA & SOC'Y, no. 5, 2006 (Can.), at 825, 831, *available at* http://sterneworks.org/mp3.pdf (last visited Oct. 19, 2012).

33. *Id.*

34. No Electronic Theft ("NET") Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amended in scattered sections of 17, 18 & 28 U.S.C).

35. Copyrights—Term Extension and Music Licensing Exemption ("The Sonny Bono Act"), Pub. L. No. 105-298, 112 Stat. 2827 (1998) (codified as amended in scattered sections of 17 U.S.C.).

36. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 5, 17, 28 & 35 U.S.C).

attacking unauthorized distribution services like Napster to an aggressive legal campaign by suing hundreds of individual file sharers each year.[37] While Hollywood justified its aggressive stance on protecting its business interests by citing billions in potential revenue lost, Internet users held different opinions.[38]

Many Internet users perceived Hollywood's aggressive litigation and legislative efforts, copyright technologies, and increased online surveillance as threats to the core principles of the Internet and, more importantly, as blatant violations of civil rights.

C. Intelligence Gathering

Governmental and corporate use of the Internet to gather information stems from several functions. First, the federal government considers the Internet a powerful tool in the war on terrorism.[39] Second, law enforcement has integrated the Internet into its investigations.[40] Third, corporations began using information collected from Internet users to further their commercial interests.[41] While these three functions can justify data collection and censorship with legitimate reasons, they have raised concerns from many Internet users.

Since the September 11, 2001, terrorist attacks on the World Trade Center, federal agencies have incorporated cyber-security as an important part of an overall terrorism strategy.[42] In 2003, the White House issued the first comprehensive strategy to secure cyberspace.[43] Specifically, the execu-

37. Kravets *File Sharing Lawsuits at a Crossroads, After 5 Years of RIAA Litigation, supra* note 24 ("[T]he Recording Industry Association of America began its massive litigation campaign that now includes more than 30,000 lawsuits targeting alleged copyright scofflaws on peer-to-peer networks.").

38. STEPHEN E. SIWEK, INST. FOR POL'Y INNOVATION, POL'Y REPORT 188: THE TRUE COST OF SOUND RECORDING PIRACY TO THE U.S. ECONOMY (2007), *available at* http://www.ipi.org/docLib/20120515_SoundRecordingPiracy.pdf; STEPHEN E. SIWEK, INST. FOR POL'Y INNOVACTION, POL'Y REPORT 186: THE TRUE COST OF MOTION PICTURE PIRACY TO THE U.S. ECONOMY (2006), *available at* http://www.ipi.org/docLib/20120117_CostofPiracy.pdf.

39. GARY CHAPMAN, THE 21ST CENTURY PROJECT, NATIONAL SECURITY AND THE INTERNET (1998), *available at* http://www.utexas.edu/lbj/21cp/isoc.htm.

40. *Id.* at 13–14.

41. *How Companies Collect Your Private Information When You Browse Online*, REPUTATION.COM, http://www.reputation.com/reputationwatch/articles/how-companies-collect-manage-and-use-your-private-information-when-you-browse-online (last visited Oct. 8, 2012).

42. *See* U.S. DEP'T OF HOMELAND SEC. COMPUTER EMERGENCY READINESS TEAM, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

43. *Id.*

tive plan under the Department of Homeland Security ("DHS") outlined cyber threats to national critical infrastructures such as banking and finance, chemical, oil and gas, electric, transportation, water, and information technology.[44]

The *National Strategy to Secure Cyberspace* was amended in 2011 by the DHS's *Blueprint for a Secure Cyber Future*.[45] The Blueprint specifies the establishment of "transparent processes," and the scope of the Blueprint seeks to fulfill the Federal Information Security Management Act of 2002.[46] This act specifies that the federal government protect security risks.[47]

According to some critics, however, such government plans do not reflect the true nature of the government's intent. In 2012, a proposed amendment to the Communications Assistance for Law Enforcement Act ("CALEA"),[48] requiring companies such as Microsoft, Facebook, Yahoo, and Google to grant the Federal Bureau of Investigations ("FBI") and other federal agencies "backdoor access" to conduct surveillance as part of larger counterterrorism operations.[49] The FBI has expanded its Internet wiretap operations under CALEA to include automated recording systems from "20 'central monitoring plants' [in 2002] . . . to 57 in 2005."[50] The growing body of legislation that threatens the erosion of Internet autonomy and disregard for civil rights has prompted the EFF to take action offline.

D. The Nature of EFF Cases

The EFF has taken on a number of cases as an Internet rights advocate, both as litigants and in supporting roles.[51] In essence, the EFF considers the online environment an extension of the physical world as reflected by the

---

44. *See id.* at 5.

45. U.S. DEPT OF HOMELAND SEC., BLUEPRINT FOR A SECURE CYBER FUTURE (2001), *available at* http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

46. *Id* at 2, 8; *see* Federal Information Security Act ("FISMA") of 2002, 44 U.S.C. §§ 3541–3549 (2012).

47. FISMA § 3547.

48. Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4278 (1994).

49. Declan McCullagh, *FBI: We Need Wiretap-Ready Web Sites—Now*, CNET.COM (May 4, 2012, 9: 24 AM), http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/.

50. Ryan Singel, *Point, Click . . . Eavesdrop: How the FBI Wiretap Net Operates*, WIRED.COM (Aug. 29, 2007), http://www.wired.com/politics/security/news/2007/08/wiretap?currentPage=all.

51. *See* ELEC. FRONTIER FOUND., *Our Work*, EFF.ORG, https://www.eff.org/work (last visited Sept. 20, 2012).

nature of cases related to the defense of threats to the fundamental rights.[52] Specifically, the organization is interested in legal issues regarding free speech, fair use of copyrighted material, technological innovation, government and corporate transparency, and the protection of privacy.[53] The EFF states on its website, "when you go online, your rights should come with you."[54]

The EFF's free speech cases often involve some form of applied online censorship.[55] In accordance with the spirit of the Internet in disseminating unfettered information, the organization considers this information as a form of journalism.[56] Such forms of speech range from content shared on social networks, such as Facebook and Twitter, to blogs and message boards.[57] According to the EFF, "preserving the Internet's open architecture is critical to sustaining free speech. But this technology capacity means little without sufficient legal protections."[58]

The EFF serves as a consumer rights advocate.[59] The two areas that serve this end are the use of copyrighted material and protection of innovative ideas.[60] The organization has fought legal battles to ensure that consumers who purchase music and other media can use it on multiple devices.[61] For example, a number of cases have targeted the Digital Millennium Copyright Act ("DMCA"), which amends Title 17 copyright law to criminalize the circumvention of copyright protection.[62] According to the EFF, this law can impact consumers by limiting the way in which media is consumed.[63] In addition, the EFF has mobilized resources to protect the creators of such

52. *See* Barlow, *supra* note 2.

53. ELEC. FRONTIER FOUND., *Our Work*, *supra* note 52.

54. ELEC. FRONTIER FOUND., *Free Speech*, EFF.ORG, https://www.eff.org/issues/free-speech (last visited Oct. 8, 2012).

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. ELEC. FRONTIER FOUND., *Free Speech*, *supra* note 54.

60. ELEC. FRONTIER FOUND., *Innovation*, EFF.ORG, https://www.eff.org/issues/innovation (last visited Oct. 8, 2012); ELEC. FRONTIER FOUND., *Intellectual Property*, EFF.ORG, https://www.eff.org/issues/intellectual-property (last visited Oct. 8, 2012).

61. *See* ELEC. FRONTIER FOUND., *Innovation*, *supra* note 61; ELEC. FRONTIER FOUND., *Intellectual Property*, *supra* note 61; ELEC. FRONTIER FOUND., *Our Work*, *supra* note 52.

62. DMCA, Pub. L. No. 105-304, 112 Stat. 2860; ELEC. FRONTIER FOUND., *2012 DMCA Rulemaking*, EFF.ORG, https://www.eff.org/2012-dmca-rulemaking (last visited Oct. 8, 2012).

63. *See* ELEC. FRONTIER FOUND., *Intellectual Property*, *supra* note 61.

tools and other technologies, considered innovators by the EFF, who are often legally intimidated by large corporations.[64]

The EFF has taken on a number of cases to defend Internet-user privacy rights against corporate and government entities.[65] For instance, web browser histories and other information stored on computers have been collected by corporate and government entities.[66] While most of this information has been collected innocuously in the name of merely targeted advertising or, more importantly, national security, the EFF warns of scenarios such as security agencies tracking an individuals' location via a cell phone, sensitive medication information being exposed between a doctor and patient, and the use of "spying or systems sabotage [on] dissidents."[67]

II. DATA AND METHODOLOGY

The data used for these analyses come from a contextual analysis of state and federal judicial decisions. "Contextual analysis [allows us to] study the role of . . . group . . . actions and attitudes" in a quantitative manner.[68] Contextual analysis is proper when a researcher wants to examine trends and characteristics of individuals belonging to a group.[69] The gathering of data through contextual analysis for this work has been condensed into one database. The dataset used for this study contains over 180 observations from 1990 to 2012. Contextual analysis of judicial decisions through contextual analysis has a longstanding history in the social sciences at all tiers of the judiciary.[70]

64. ELEC. FRONTIER FOUND., *Innovation*, *supra* note 61.

65. ELEC. FRONTIER FOUND., *Privacy*, EFF.ORG, https://www.eff.org/issues/privacy (last visited Oct. 8, 2012).

66. *Id.*

67. *Id.*

68. Gudmund R. Iversen, *Contextual Analysis*, *in* QUANTITATIVE APPLICATION IN THE SOCIAL SCIENCES at 3, 3 (Sage Publ'ns issue 7, pt. 81, 1991).

69. *Id.*

70. *See*, ROBERT A. CARP & CHARLES K. ROWLAND, POLICYMAKING AND POLITICS IN THE FEDERAL DISTRICT COURTS 8, 16 (1983) (discussing contextual analysis of decisions at the trial court level); Kenneth M. Dolbeare, *The Federal District Courts and Urban Public Policy: An Exploratory Study*, *in* FRONTIERS OF JUDICIAL RESEARCH 373, 374–75 (Joel B. Grossman et al. eds., 1968) (discussing contextual analysis of decisions at the trial court level); Jeffrey A. Segal, *Supreme Court Justices as Human Decision Makers: An Individual-Level Analysis of Search and Seizure Case*, 48 J. POL., no.4, 1986, at 938, *available at* http://www.jstor.org/stable/21310006 (discussing contextual analysis of decisions by courts of last resort); Donald R. Songer, *Consensual and Nonconsensual Decisions in Unanimous Opinions of the United States Courts of Appeals*, 26 AM. J. POL. SCI., no. 2, 1982, at 225, 225, *available at* http://www.jstor.org/

A. Endogenous Variable

Each observation consists of a jury or judge decision, coded as either successful or not successful to form the endogenous variable. Decisions were coded as successful when the adjudicator found in favor of the position the EFF was advocating on behalf of and unsuccessful when the adjudicator did not find in favor of the position advocated by the EFF. Cases where the result is still pending or the party withdrew before non-interlocutory adjudication are included in the database for completeness but are not included in the analyses.

B. Exogenous Variables

The Amicus variable refers to the role played by the EFF. It has been coded as 0 when the EFF is counsel for a party and 1 when the EFF is in the role of amicus curiae or an amici.

The Party variable refers to the legal position of the party with whom the EFF is involved. It has been coded as 0 for Defendant and 1 for Plaintiff.

The Tier variable refers to the judicial tier with which the EFF is engaged. It has been coded as 1 for trial courts, 2 for courts of appeal, 3 for supreme courts. Instances where the EFF was involved in multiple tiers of the same case have each been coded as separate observations.

The Jurisdiction variable refers to whether the case falls under State or Federal jurisdiction. It has been coded as 0 for State and 1 for Federal.

The Circuit variable refers to the circuit in which the case is being heard. It has been coded in accordance with the regional numerical designations assigned by Congress as 1 to 13.

The Case Type variable refers to the underlying issues in the case. It has been coded in the following manner:

0 = Free speech Issues

1 = Copyright and general intellectual property issues

2 = Privacy and spying issues

3 = Digital Millennium Copyright Act ("DMCA") and innovation cases

To examine these variables, we have utilized correlations. A "[c]orrelation is a statistical technique that can show whether and how strongly pairs of variables are related."[71] "Correlations can [also] tell you just how much of the variation in [one variable] is related to [the other]."[72] Correlations additionally show whether the data contain unsuspected correlations, which makes it ideal for this examination.[73] Correlation coefficient

stable/2111037 (discussing contextual analysis of decisions at the appellate court level).

71. *Correlation*, SURVEYSYSTEM.COM, http://www.surveysystem.com/correlation.htm (last visited Oct. 8, 2012).

72. *Id.*

73. *Id.*

significance has been reported to highlight strong relationships between variables in this examination.

III. ANALYSES

In general, the EFF is a successful advocate for Internet anonymity with a success rate of 76.8%. This suggests that the EFF is being very careful in the cases they take and utilizing their resources efficiently. It also makes it more difficult for the various crime prevention entities to police the behavior of suspected wrongdoers, opening avenues for further crime and security issues.

TABLE ONE: EFF WORKLOAD

Free Speech	37% (N=67)
Intellectual Property	31.5% (N=57)
Privacy	18.8% (N= 34)
DMCA	7.3% (N=13)
Other	5.4% (N=9)

These results are not an artifact of their workload. As Table One (above) shows, their workload is nicely divided with an emphasis on free speech and intellectual property cases.

As Table Two (below) shows, the data reveals some striking correlations. Most significantly, when the EFF acts in the role of amicus they achieve their greatest success at the top tier courts. This suggests that the best role for the EFF is to not directly represent parties as they have in many cases, but to focus on the pending litigation and get involved at the later steps of the process.

TABLE TWO: CORRELATIONS

	Successful	Amicus	Party	Tier	State/Federal	Case Type
Amicus	.045					
	.671					
Party	-.136	-.080				
	.191	.352				
Tier	-.140	.440	.197			
	.184	.000**	.018*			
State/Federal	.163	.107	-.045	.011		
	.121	.243	.610	.904		
Case Type	.078	.099	-.047	.118	.174	
	.453	.243	.572	.155	.046*	
Circuit	-.036	.047	.006	.172	.029	.006
	.734	.581	.939	.036*	.743	.940

TABLE 4: PERCENTAGE LIBERAL DECISIONS IN CIVIL LIBERTIES AND RIGHTS CASES BY REGION, 1928–2003

	North		*South*		
Year	%	n	%	n	T test
1928	60	(20)	100	(2)	-1.10
1932	65	(38)	33	(3)	1.11
1936	32	(89)	16	(6)	.80
1940	37	(129)	33	(15)	.34
1944	39	(208)	37	(45)	2.69**
1948	43	(217)	40	(42)	.39
1952	42	(222)	48	(50)	-.67
1956	46	(439)	31	(64)	2.36*
1960	38	(280)	35	(101)	.51
1964	38	(231)	42	(169)	-.82
1968	35	(422)	44	(277)	-2.37*
1972	53	(1255)	58	(744)	-2.18*
1976	49	(1508)	39	(777)	4.70**
1980	51	(1383)	45	(564)	2.72**
1984	47	(1453)	44	(540)	1.32
1988	43	(2244)	41	(826)	1.30
1992	39	(1898)	37	(603)	1.12
1996	38	(3085)	30	(1259)	5.29**
2000	38	(1450)	34	(543)	1.66

* Significant at <.05
** Significant at <.01

Table Two also shows that, when acting on behalf of the plaintiff, the EFF is more successful than when acting on behalf of the defendant, especially in the top tier courts. Though this may be an artifact due to client selection, it also suggests that when acting in state courts that are mired in cases regarding tort, crime, domestic issues, and contracts, the EFF can be successful due to their adversary's inexperience with the complexity of the issues at hand. To provide a greater level of security protection for the Internet, practitioners may want to conduct workshops and continuing legal education classes on these issues to dilute the success of groups like the EFF.

Table Two also shows that certain case types are more successful in federal versus state courts. We feel this is due to the nature of jurisdiction requiring most intellectual property cases, 31.5% of the cases analyzed, falling under exclusive federal jurisdiction. However, when the EFF does act on behalf of a party in state court, they are successful 100% of the time in 25 observations. This may suggest that the subject matter of the cases going to state court are the types of cases, such as privacy and DMCA cases, that can be tilted in a more liberal direction by groups such as the EFF, possibly opening the Internet to further access by terrorists and other security risks.

IV. CONCLUSION AND CALL FOR FUTURE RESEARCH

This paper shows that Internet freedom and security are not insulated from the social, political, and perhaps more importantly, legal realities of the physical world. Internet rights advocacy groups, despite their declaration that cyberspace is a separate, free space where one can express pure ideas

and thoughts in unfettered discourse, must defend those rights in more traditional forums, such as through legislation and in the courts.

Our findings show that one such group, the EFF, has been relatively successful in defending issues of consumer rights. This success, however, may reflect legal strategies based on a selection of cases in certain jurisdictions. Their legal victories are significant when considering their limited resources, as reflected by the heavy use of amicus briefs.

The EFF's stance on Internet freedom has created friction with law enforcement and some commercial entities that have divergent definitions and understandings of security. For many government agencies, including federal law enforcement, privacy comes at the cost of security, where terrorist groups can potentially communicate and plan attacks without the threat of detection.[74] Former FBI legal representative Valerie Caproni explains that backdoor access to websites is essential for security operations, stating that the FBI is "'increasingly unable'" to access "'[w]eb-based e-mail, social-networking sites, and peer-to-peer communications.'"[75]

Our basic assessment of the EFF's legal strategies serves as a preliminary starting point in exploring issues in Internet freedom and security. Future research can explore areas of case selection strategies that include issues of importance and specific legal strategies using more in-depth case analysis.

74. McCullagh, *supra* note 50.

75. *Id.*