Pace Law Review

Volume 32
Issue 3 *Summer 2012*

Article 8

June 2012

Playing the Mysterious Game of Online Love: Examining an Emerging Trend of Limiting § 230 Immunity of the Communications Decency Act and the Effects on E-Dating Websites

Matthew Altenberg
Villanova University School of Law

Playing the Mysterious Game of Online Love: Examining an Emerging Trend of Limiting § 230 Immunity of the Communications Decency Act and the Effects on E-Dating Websites

Matthew Altenberg*

"If I would like to make myself seem more attractive to the opposite sex . . . I don't go and get a new haircut, I update my profile. That's just the way it is, you know."[1]

I. Introduction

Online dating has proliferated in America, making it statistically more likely that a single adult American will find their future mate online than in a bar, work, or school.[2] In the United States alone, over fifteen hundred dating social-lifestyle websites exist, attracting over twenty-five million users per month.[3] Worldwide, that number soars to over 122 million

*J.D. Candidate, 2013, Villanova University School of Law.

1. *He's Just Not That Into You Script – Dialogue Transcript*, SCRIPT-O-RAMA.COM, http://www.script-o-rama.com/movie_scripts/h/hes-just-not-that-into-you-script.html (last visited June 9, 2012).

2. *See* Michael J. Rosenfeld, *How Couples Meet and Stay Together*, STANFORD UNIV. SSDS SOCIAL SCI. DATA COLLECTION (Sept. 22, 2009, 7:02 AM), http://data.stanford.edu/hcmst (reporting findings of studies of how Americans meet their spouses showing that the Internet has become the predominant source of how people initially meet); *see also* Cristen Conger, *5 Fundamental Truths of Online Dating*, HUFFINGTON POST (Feb. 24, 2011, 4:40 PM), http://www.huffingtonpost.com/cristen-conger/online-dating-facts_b_823816.html (describing Stanford University survey data).

3. *See* Julie Spira, *The Business of Love*, HUFFINGTON POST (June 29, 2011, 4:24 PM), http://www.huffingtonpost.com/julie-spira/the-business-of-love_b_885780.html (citing the number of dating websites and monthly users, and concluding that online dating is a lucrative emerging business in

users who log onto dating websites monthly.[4] Given these statistics, many issues arise concerning e-dating legitimacy, safety, and reliability.[5]

Online dating websites exist on the ever-evolving Internet, which consists of privately owned servers that facilitate e-media platforms like Match.com.[6] These privately owned websites are some of the intermediaries to which § 230 of the Communications Decency Act provides immunity concerning third-party speech on their services.[7] Section 230 has provided clarity for online intermediaries, while "[stopping] judicial attempts to adapt the common law" to the rapidly developing world of e-media platforms on the Internet.[8]

This Comment argues that limiting the application of § 230 into a narrower shield of immunity, rather than a broad blanket shield, is consistent with the legislative intent underlying § 230. Part II provides a background of intermediaries, both in the traditional sense and in the twenty-first century Internet-based sense. Part III outlines the

America); *see also* Mark Brooks, *How Has Online Internet Dating Changed Society?*, ONLINE PERSONALS WATCH (Jan. 2011), *available at* http://www.onlinepersonalswatch.com/files/idea-white-paper-final-review-copy-only-updated-1-19-2.pdf (describing the number of worldwide users of Internet dating websites and the increase in monthly users).

4. *See generally* Brooks, *supra* note 3 (reporting increase in worldwide users of Internet dating websites).

5. *See* Conger, *supra* note 2, at pt. 2 (explaining that Internet dating profiles are "riddled with white lies" and users must approach Internet dating like interviews because of safety concerns); *see also Online Dating Sites Sued For Fraud*, SAVVY INSIDER (Sept. 7, 2011, 7:05 PM), http://www.savvyinsider.com/article.php?op=viewArticle&article_ID=427.

6. *See* Fredrick Oduol Oduor, *The Internet and Copyright Protection: Are We Producing a Global Generation of Copyright Criminals?*, 18 VILL. SPORTS & ENT. L.J. 501, 502 (2011) (noting how the Internet has "changed several perceptions" concerning how people conduct "personal . . . affairs" in their lives, which has led to "depersonalization"). *See generally* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 382-83 (2010) (describing Internet servers and e-media platforms and how they interact with each other).

7. *See* Ardia, *supra* note 6, at 411 (outlining what Internet intermediaries may claim under § 230 immunity).

8. *See id.* (noting that § 230 has been very useful in developing clear guidelines to online intermediaries concerning liability, which common law principles failed to do).

constitutional framework concerning free speech and intermediaries. Part IV explains the development and application of § 230. Additionally, Part IV introduces new case law that represents the emerging trend of limiting § 230 immunity. Part V analyzes two significant cases that establish this trend. Additionally, Part V argues that a limited § 230 immunity application is within the proper scope of congressional findings and purpose set-forth in § 230. Finally, Part VI concludes by examining the impact the emerging trend will have on e-dating and other lifestyle social networking websites.

II. Background Of Intermediaries

The Internet is a network of networks.[9] The networks on the Internet incorporate various electronic links, each of which originate from a user and connect to a server, to a router, and ultimately to an Internet Service Provider ("ISP").[10] The Internet user relies upon electronic links or organizational directories, like the Google search-engine, to find specific information from an endless amount of stored data.[11] These links between speaker and listener make up Internet intermediaries, which range from search engines to private websites.[12] The legal definition of an intermediary is "[a] mediator or go-between; a third- party negotiator."[13] Additionally, an online intermediary is defined as any entity that enables the communication of information or data from one user to another user.[14]

9. *See generally* Seth Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 16 (2006) (explaining the background of the Internet and how networks developed within it).

10. Kreimer, *supra* note 9, at 17-20.

11. *Id.* at 18 (highlighting the process of data storage on the Internet and how users rely on organizational directories to find specific data or websites).

12. *See generally* Ardia, *supra* note 6, at 385-87 (discussing various types of Internet intermediaries, which include communication conduits, content host, and search/application providers).

13. BLACK'S LAW DICTIONARY 890 (9th ed. 2009).

14. *See, e.g.*, Ardia, *supra* note 6, at 385 (noting differences between

The development of communication intermediaries began in the eighteenth century, when the optical telegraph transmitted messages across Europe.[15] Following the optical telegraph, the electric telegraph, which was termed the "Victorian Internet," revolutionized how humans communicated.[16] Through this historical development, private online intermediaries emerged by a communication process of common languages called the Transfer Control Protocol/Internet Protocol ("TCP/IP"), which allows computers running on different operating systems to communicate with each other.[17]

Today, these interconnected networks create a variety of platforms for speech and press, which include e-dating websites, social networking websites, photo-hosting services, and blogs.[18] Although the Internet has no central authority, the decentralized structure has led to the proliferation of the Internet as a communication tool.[19] Due to the decentralized structure, private intermediaries have flourished in the "industrial information economy," which provides users with a wide range of communication possibilities, including e-dating.[20]

traditional intermediaries and online intermediaries).

15. *See* TOM STANDAGE, THE VICTORIAN INTERNET: THE REMARKABLE STORY OF THE TELEGRAPH AND THE NINETEENTH CENTURY'S ON-LINE PIONEERS 12 (1998) (discussing historical background of the telegraph and the development of communication through electronic means).

16. *Id.* at 16.

17. *See generally* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 821 (2004).

18. *See* Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115, 1116 (2005) (detailing a vast amount of private entities on the Internet that are under the U.S. Constitution's free speech protection); *see also* Yang-Ming Tham, Comment, *Honest to Blog: Balancing the Interests of Public Figures and Anonymous Bloggers in Defamation Lawsuits*, 17 VILL. SPORTS & ENT. L.J. 229, 234 (2010) (noting the difficulty in classifying online blogs as writings or free press because online blogs are a "recent innovation").

19. *See generally* Jack M. Balkin, *Media Access: A Question of Design*, 76 GEO. WASH. L. REV. 933, 936-39 (2008) (describing the importance of the Internet as a communication tool and how its decentralized structure has allowed exponential growth of Internet intermediaries).

20. *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 32 (2006), *available at* http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf (explaining how

A. *Intermediary Classifications*

The functions of e-intermediaries are not as straightforward as traditional intermediaries, and the illustration below highlights the role that various intermediaries play when an Internet user requests data.[21] When an Internet user requests a profile page from an e-dating website, the profile page request is sent from the original user's computer to a computer network run by an ISP.[22] Next, the ISP sends the profile data request via multiple intermediaries owned by the ISP that enable peering connections to that person's network.[23] From this point, the data is sent from the e-dating websites server, which hosts the profile data, to the original user who sent the data request.[24] From this example, intermediaries can be grouped into three categories, each discussed below: 1) Communication Conduits; 2) Search/Application Providers; and 3) Content Hosts.[25]

the "industrial information economy" has transformed the global landscape regarding how communication is transferred and how private intermediaries have played a central role in this transformation); *see also* Steven Masur, *Collective Rights Licensing for Internet Downloads and Streams: Would it Properly Compensate Rights Holders?*, 18 VILL. SPORTS & ENT. L.J. 39, 39-40 (2011) (highlighting how the Internet has changed business models concerning digital media rights and noting that copyright law had to be reexamined due to the proliferation of Internet intermediaries allowing consumers to download music online). *See generally* Solum & Chung, *supra* note 17, at 847-49.

21. *See* Ardia, *supra* note 6, at 386 (examining the process an intermediary plays when users request data from private websites and how different intermediaries are required when one Internet user requests data).

22. *See id.* at 386-87.

23. *See generally* Paul Milgrom et al., *Competitive Effects of Internet Peering Policies, in* THE INTERNET UPHEAVAL: RAISING QUESTIONS, SEEKING ANSWERS IN COMMUNICATIONS POLICY 175, 175-80 (Ingo Vogelsang & Benjamin Compaine eds., 2000) (describing "peering connections" as a process in which neither party pays for content exchanged between ISPs—instead the ISP collects revenue from the original user).

24. *See* Ardia, *supra* note 6, at 386-87.

25. *See id.* at 387.

1. Communication Conduits

First, communication conduits are intermediaries that facilitate the transportation of data across an Internet network.[26] This type of intermediary takes the form of an Internet provider, which is usually provided through a telephone, cable, or satellite company.[27] The Internet provider allows users to access the Internet, and most Internet providers have a contractual relationship with the user who pays for Internet service.[28] In comparison to traditional intermediaries, content intermediaries may be analogized to newspaper delivery people or telephone companies that deliver voice traffic.[29] Finally, communication conduits do not have direct knowledge of the data they are transporting—thus, their primary role is the transportation of the requested data.[30]

2. Application and Search Providers

Second, application and search providers are intermediaries that provide access to Internet data by organizing and filtering the data.[31] Application and search provider intermediaries enable Internet users to find specific data from an endless amount of data available on the Internet.[32] Two examples of application and search provider intermediaries are the Google and Yahoo search engines.[33] In comparison to traditional intermediaries, application and search provider intermediaries may be analogized to a

26. *See id.* at 386-87.

27. *See id.*

28. *See id.* (noting that ISPs are one type of intermediary involved in the process when a user requests data on the Internet).

29. *See id.* (comparing communication conduits to traditional intermediaries to illustrate the complexity of e-intermediaries).

30. *See id.*

31. *See id.* at 389.

32. *See id.* (noting the importance that application and search provider intermediaries play, because the amount of data available online is massive and organization of that data enables users to filter out data that they are looking for).

33. *See id.* at 388.

telephone directory or a stock price index.[34]

3. Content Hosts

Third, content host intermediaries store, cache, and provide access to third-party content.[35] Content host intermediaries are primarily privately owned websites.[36] For example, when group users gather on Match.com to find a potential mate, Match.com plays host to third party speech through the terms and conditions set-forth by Match.com.[37] In comparison to traditional intermediaries, content hosts may be analogized to book stores or libraries.[38] This Comment will focus on content hosts in examining the effects of a narrower § 230 immunity.

B. *Liability of Intermediaries*

Traditionally, intermediaries are not liable as primary malfeasors, however, they may be liable through secondary liability.[39] Primary liability arises from the original speaker, and secondary liability arises from an actor that has a nexus to the original speaker.[40] Typically, online intermediaries have

34. *See id.* at 389.

35. *See id.* at 387.

36. *See id.* at 387-88 (stating that servers owned by private companies enable the storage of third party content and that this type of intermediary makes up the most commonly thought-of Internet intermediary).

37. *See id.* (citing examples of content host intermediaries such as Facebook.com, Flickr.com, and Youtube.com).

38. *See id.* at 388-89 (describing offline distributor intermediaries as similar to content hosts, in that they facilitate third party speech distribution to reach a broad audience).

39. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 278-81 (1964) (holding that the intermediary of a newspaper was safeguarded by the First and Fourteenth Amendments in a libel action against a public official); Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162-63 (2d Cir. 1971) (vicarious liability and contributory liability, in the intellectual property context, applies when a party with knowledge of infringing activity induces or causes the infringing conduct of another). *See generally* Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 912-16 (2002).

40. *See Gershwin Publ'g Corp.*, 443 F.2d at 1162-63 (defining contributory liability, within the intellectual property field, as having

various legal protections, like § 230 immunity, which protects online intermediaries from secondary liability, unless they act in a manner indicating that they "knew or should have known" about the illegal action.[41] Additionally, § 230 excludes intellectual property law, federal criminal law, and communications privacy law.[42] Therefore, the main form of liability relevant to intermediaries that fall outside of § 230 immunity are speech based torts, such as misrepresentation or defamation.[43]

Generally, content hosts are not liable for the content they provide to other users unless they have "knowledge" that it is illegal.[44] When a content host intermediary gains "knowledge" that the data or material it is distributing is illegal in nature, it is required to stop making the data available, or it will face liability.[45] This type of "knowledge" may be defamatory on its face, or inferred from past actions.[46] However, if a content host intermediary is under a duty to the public to accept and transmit messages, then knowledge alone is insufficient to

knowledge of infringing activity or materially contributing to infringing conduct); Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257, 1263 (N.D. Cal. 2006) (explaining that § 230 immunity did not absolve Yahoo! from liability when it deliberately and intentionally created false profiles for the purpose of luring clients to renewing subscriptions on e-dating service). *See generally* Reinier H. Kraakman, *Corporate Liability Strategies and the Costs of Legal Controls*, 93 YALE L.J. 857, 889-93 (1984) (discussing the act of aiding and abetting as an act creating secondary liability in criminal law, where intermediaries are not required to act affirmatively, but must only act not to aid a known illegal act).

41. *See Gershwin Publ'g Corp.*, 443 F.2d at 1162 (explaining that liability may arise when the intermediary knew that the content was illegal).

42. 47 U.S.C. § 230(e) (2006) (listing the types of law not included within § 230 immunity).

43. *See* Hamdani, *supra* note 39, at 916 (noting that the main forms of liability concerning § 230 lawsuits are libel, defamation, and misrepresentation).

44. *See* Tacket v. Gen. Motors Corp., 836 F.2d 1042, 1046 (7th Cir. 1987); Lerman v. Flynt Distrib. Co., 745 F.2d 123, 139 (2d Cir. 1984); Dworkin v. Hustler Magazine, Inc., 634 F. Supp. 727, 729 (D. Wyo. 1986) ("[O]ne who only delivers or transmits defamatory matter published by a third person is subject to liability if . . . he knows or had reason to know of its defamatory character." (quoting RESTATEMENT (SECOND) OF TORTS § 581 (1977)).

45. *See Dworkin*, 634 F. Supp. at 729.

46. *See Tacket*, 836 F.2d at 1046.

establish liability.[47] Thus, a content host intermediary assumes the sender is privileged unless it has an affirmative reason to know of information to the contrary.[48] Therefore, content host intermediaries not classified as a "public utility" are afforded the standard of "know or have reason to know" of a misrepresentation or falsity.[49]

III. Constitutional Framework of First Amendment Protections

In the 1960s, the U.S. Supreme Court established a background for evaluating sanctions on intermediaries,[50] and as Seth Kreimer notes "[t]hese doctrines continue to frame the rights of litigants in modern litigation over efforts . . . of Internet communications . . . ."[51] The first two cases involved intermediary protection for booksellers when state statutes made it illegal for booksellers to sell or display obscene or objectionable books.[52] During this time, the Supreme Court stated that the First Amendment does not support strict

47. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 278-81 (1964); Nat'l Ass'n of Regulatory Util. Comm'rs v. Fed. Commc'n Comm'n, 533 F.2d 601, 608 (D.C. Cir. 1976); *Dworkin*, 634 F. Supp. at 729-30.

48. *See* O'Brien v. W. Union Tel. Co., 113 F.2d 539, 543 (1st Cir. 1940).

49. *See* Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 993 (2005); *Dworkin*, 634 F. Supp. at 729.

50. *See, e.g.*, *N.Y. Times Co.*, 376 U.S. at 290-92 (holding that First Amendment protections apply to intermediaries, and that public official seeking damages for libel must prove by clear and convincing evidence that defendant published statements with actual malice); Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 71 (1963) (invalidating a state practice that notified distributors that certain magazines and books were found to be objectionable for display or sale on the grounds that the published items were obscene or indecent to minors)

51. Kreimer, *supra* note 9, at 51.

52. *See* Smith v. California, 361 U.S. 147, 151, 154 (1959) (declaring unconstitutional a city ordinance that made it illegal for bookstore operators to have obscene books on their shelves because the ordinance had "the collateral effect of inhibiting the freedom of expression" and because the censorship effect of the ordinance through intermediaries would be "censorship affecting the whole public"); *Bantam Books, Inc.*, 372 U.S. at 64 n.6 ("The constitutional guarantee of freedom of the press embraces the circulation of books as well as their publication . . . ." (citing Lovell v. City of Griffin, 303 U.S. 444, 452 (1938))).

liability on intermediaries.[53] In *Bantam Books, Inc. v. Sullivan*, the Court stated that First Amendment protections are afforded to the publication and distribution of speech.[54] Additionally, the Court in *Bantam Books, Inc.* found that acts and practices that "directly and designedly stopped the circulation of publications" have the effect of suppressing speech by condemning intermediaries that distribute the books.[55]

In *New York Times Co. v. Sullivan*, the Court stated that the First Amendment protection extends to intermediaries.[56] Damages for defamatory speech must be "prove[n]by clear and convincing evidence that the defendant published the defamatory statement with actual malice . . . ."[57] The Court noted that "'actual malice' . . . is, with knowledge that it was false or with reckless disregard of whether it was false or not." "[58] Additionally, the Court looked at New York Times Co. as a whole concerning "knowledge," rather than focusing on the individual publisher within the New York Times Co.[59] With this doctrinal overview of Supreme Court precedent concerning traditional intermediaries, § 230 may be thought of as a continuation of intermediary protection in the twenty-first century.[60]

IV. The CDA and § 230 Immunity

This Section will provide an overview of § 230, including the congressional history of the legislation, case law applying the traditional blanket immunity of § 230, and case law representing the emerging trend of limiting the application of §

53. *See Smith*, 361 U.S. at 154 (finding that a city ordinance dispensing of the scienter-knowledge requirement for sellers of books containing obscene material could not stand due to First Amendment protections).

54. *Bantam Books, Inc.*, 372 U.S. at 72.

55. *See id.* at 68 (the practice of intermediary censorship has the effect of suppressing speech protected by the First Amendment).

56. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 290-92 (1964).

57. Masson v. New Yorker Magazine, Inc., 501 U.S. 496, 510 (1991) (citing *N.Y. Times Co.*, 376 U.S. at 279-80).

58. *N.Y. Times Co.*, 376 U.S. at 280.

59. *See id.* at 290-91.

60. *See* Kreimer, *supra* note 9, at 55.

230 immunity. Subsection A will provide an overview of the development of § 230. Subsection B will discuss a test courts have developed when determining when to apply § 230 immunity. Subsection C will describe a variety of cases applying § 230 with the developed test under a blanket immunity application. Finally, Subsection D will explain the case law that represents the emerging trend that has limited the application of § 230 immunity.

A. *The Development of § 230*

Senator James Exon introduced an amendment attempting to regulate Internet speech, which later turned into the Communications Decency Act ("CDA") on February 1, 1995.[61] Senator Exon wanted to keep the Internet from becoming a "red light district" and he wanted to better protect families and children from those individuals who "cruise the digital world [seeking] to engage children in inappropriate communications and introductions."[62] According to Senator Exon the CDA was intended to protect children from indecency online.[63]

However, after Senator Exon introduced the CDA, there were "strong objections from the interactive computer service industry."[64] The computer service industry claimed that they would have to screen and monitor an immense amount of data to protect children, which was claimed to be "an impossible task."[65] Thus, defenses were added to the proposed legislation to narrow its reach.[66] Representatives Cox and Wyden, who

61. *See* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 52 (1996) (describing Senator Exon's intent in introducing CDA).

62. 141 CONG. REC. S1953 (daily ed. Feb. 1, 1995) (statement of Sen. James Exon).

63. 141 CONG. REC. S8089 (daily ed. June 9, 1995) (statement of Sen. James Exon).

64. *See* Cannon, *supra* note 61, at 59.

65. *See id.* at 59-61 (listing the defenses the computer industry advocated for concerning the reach of the CDA).

66. 141 CONG. REC. S8345 (daily ed. June 14, 1995) (statement of Sen. Dan Coats) ("[I]t is the intent of this legislation that persons who are providing access to or connection with [the] Internet or other electronic service not under their control are exempted under this legislation"); *see also*

opposed the CDA, introduced a defense provision, which later became § 230 of the CDA.[67] Known as the Online Family Empowerment Amendment, the goal of the Amendment was to "promote the continued development of the Internet and. . . [to] preserve the vibrant and competitive free market that exists on the Internet . . . ." [68]

B. *The Completed Act with § 230*

The CDA, along with § 230, was passed by Congress and signed by former President Bill Clinton on February 8, 1996.[69] Under the heading "Protection for the 'Good Samaritan' Blocking and Screening of Offensive Material," § 230(c)(1) of the CDA states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[70] Although § 230(c)(1) does not explicitly state the

142 CONG. REC. H1158 (daily ed. Feb. 1, 1996) (statement of Rep. Henry Hyde) ("[t]he conference report expressly provides an absolute legal defense to any on-line access provider . . . 'solely for providing access . . . to or from a facility, system or network not under that person's control,' so long as that person is not involved in 'the creation of the content of the communication'"); 142 CONG. REC. S714 (daily ed. Feb. 1, 1996) (statement of Sen. James Exon) ("[C]omputer services such as CompuServe . . . that provide access to sites on [the] Internet which they do not control, are not liable."); 142 CONG. REC. S714 (daily ed. Feb. 1, 1996) (statement of Sen. James Exon):

> [T]he legislation generally does not hold liable any entity that acts like a common carrier without knowledge of messages it transmits or hold liable an entity which provides access to another system over which the access provider has no ownership of content. Just like in other pornography statutes, Congress does not hold the mailman liable for the mail that he/she delivers.

Id.

67. *See* 141 CONG. REC. H8468-69 (daily ed. Aug. 4, 1995).

68. *See id.*

69. *See* Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 47 U.S.C.) (stating date passed by Senate, House, and signed by President); 142 CONG. REC. S687 (daily ed. Feb. 1, 1996) (statement of Sen. Dan Coats.

70. 47 U.S.C. § 230(c)(1) (2006). Subsection (c) states in full:

term "immunity," most courts have applied the term "immunity" to §230(c)(1) and applied the effect of broad immunity.[71]

After § 230 became effective, courts developed a three-tiered test in determining whether § 230 immunity applied.[72] The first tier asks if the party claiming immunity is a "provider or user of an 'interactive computer service.'"[73] The second tier asks if the party claiming immunity is being treated as "publisher or speaker" of the content at issue.[74] The third tier asks if the content at issue is "information provided by another

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
> (1) Treatment of publisher or speaker: No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> (2) Civil liability: No provider or user of an interactive computer service shall be held liable on account of:
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Id. § 230(c)(1), (2).

71. *See, e.g.*, Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1173-76 (9th Cir. 2009); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008); Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 670-72 (7th Cir. 2008); Doe v. GTE Corp., 347 F.3d 655, 659-63 (7th Cir. 2003); Ben Ezra Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 984-87 (10th Cir. 2000).

72. *See Zango, Inc.*, 568 F.3d at 1177-78; *Craigslist, Inc.*, 519 F.3d at 671-72; *GTE Corp.*, 347 F.3d at 659-62; *Roommates.com*, 521 F.3d at 1162; Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) (stating that § 230(c) provides broad immunity for published content provided by a third party).

73. *See Ben Ezra, Weinstein, & Co.*, 206 F.3d at 985-86 (10th Cir. 2000). The definition of ICS under §230(f) is "[a]ny information service, system, or access software provider that provides or enables computer access by multiple users to a computer server . . . ." 47 U.S.C. § 230(f)(2) (2006).

74. *See* Green v. Am. Online, 318 F.3d 465, 470-71 (3d Cir. 2003).

information content provider."[75]

Additionally, within § 230 the term "interactive computer service" ("ICS") is defined as "[a]ny information service, system, or access software provider that provides or enables computer access by multiple users to a computer server . . . ."[76] The term "information content provider" ("ICP") refers to "[a]ny person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[77] Within § 230's provisions, courts have relied upon congressional findings and the policy underlying § 230 in applying immunity broadly.[78] Additionally, critics to a narrow interpretation of § 230 have noted that the objectives of § 230 are to promote, preserve, and

75. *See* Batzel v. Smith, 333 F.3d 1018, 1037 (9th Cir. 2003).

76. 47 U.S.C. § 230(f)(2).

77. *Id.* § 230(f)(3).

78. *See generally* Claudia G. Catalano, Annotation, *Validity, Construction, and Application of Immunity Provisions of Communications Decency Act, 47 U.S.C. § 230*, 52 A.L.R. FED. 2D 37 (2011) (finding that courts have applied § 230(c) immunity in a broad-based approach). Catalano notes that the findings of § 230 provide for a broad degree of immunity because the Internet has become an integral feature of our society. *See id.* at 40-42 (applying findings stated within text of the CDA). The CDA § 230 findings reads in full:

> (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represents an extraordinary advance in the availability of educational and informational resources to our citizens.
> (2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.
> (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
> (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.
> (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

47 U.S.C § 230(a)(1)-(5) (2006).

encourage the development of the Internet, which is exactly what a broad-based immunity provision accomplishes.[79]

C. *The Application of § 230*

The first Internet intermediary to be sued as an intermediary distributor occurred in *Cubby, Inc. v. CompuServe*.[80] In *Cubby*, the court relied upon the analysis in *Smith v. California*,[81] and held that CompuServe was a distributor and could not be held liable for defamatory statements in its forum unless the plaintiff could prove CompuServe "knew or had reason to know" of defamatory content.[82] The court looked at CompuServe's contract with the third-party and the time frame in which it loaded and

79. *See generally* Catalano, *supra* note 78, at 51 (describing policy aspects of CDA § 230 as encouraging broad-based immunity). The policy provisions of § 230 reads in full:

> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

47 U.S.C. § 230(b)(1)-(5) (2006).

80. *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (noting that CompuServe was treated like a distributor in the traditional common law doctrine); *see also* Anthony J. Sassan, Cubby, Inc. v. Compuserve, Inc.*: Comparing Apples to Oranges: The Need for a New Media Classification*, 22 SOFTWARE L.J. 820, 823 (1992).

81. 361 U.S. 147 (1959).

82. *See Cubby, Inc.*, 776 F. Supp. at 139-40.

presented data onto its service in deciding that CompuServe was an intermediary.[83]

1. Interactive Computer Service ("ICS")

The courts in the following cases held that the online entity was an ICS, thus, § 230 applied. In *DiMeo v. Max*,[84] the court determined that an operator of a website that hosted an online message board was an ICS.[85] In *Cornelius v. DeLuca*,[86] the court found the defendant to be an ICS because the defendant was required to access the Internet to exist and to be used by the public.[87] In *Barrett v. Fonorow*, the court found that a web site operator was a provider or user of an ICS in which the service is a message board where authors post articles.[88] In *Donato v. Moldow*, the court found that a website that hosted a bulletin board for the community was within the scope of an ICS because it used the web sites' electronic host to access the Internet.[89]

The courts in the following cases held that the online entity was not an ICS, thus, § 230 did not apply. In *Novartis Vaccines and Diagnostics, Inc. v. Stop Huntingdon Animal Cruelty USA, Inc.*, the court determined that the website operator was not an ICS because the website only posted employee information and a calendar of events.[90] In *Huntingdon Life Science, Inc. v. Stop Huntingdon Animal Cruelty USA, Inc.*, the court held that immunity was not applicable because the defendant's website simply published accounts of demonstrations and the website owner posted some newspaper articles.[91]

83. *See id.* at 140 (noting the relationship that CompuServe had with the third party who supplied defamatory information).

84. 433 F. Supp. 2d 523, 530 (E.D. Pa. 2006).

85. *See id.* at 531-32.

86. 709 F. Supp. 2d 1003, 1010 (D. Idaho 2010).

87. *Id.* at 1022.

88. *See* Barrett v. Fonorow, 799 N.E.2d 916, 922-25 (Ill. App. Ct. 2003).

89. *See* Donato v. Moldow, 865 A.2d 711, 718-21 (N.J. Super. Ct. App. Div. 2005).

90. *See* Novartis Vaccines & Diagnostics, Inc. v. Stop Huntington Animal Cruelty USA, Inc., 50 Cal. Rptr. 3d 27, 39-40 (Ct. App. 2006).

91. *See* Huntington Life Sci., Inc. v. Stop Huntington Animal Cruelty

2. Publication

The courts in the following cases held the publication requirement of § 230 was satisfied. In *Miles v. Raycom Media, Inc.*, the court held that § 230 of the CDA required publication of defamatory content.[92] Further, when a news article is put on a website which allows users to comment on the article, the website owner may qualify for immunity.[93] Additionally, in *Faegre & Benson, LLP v. Prudy*, the court found that content was published when a third-party posted allegedly defamatory content on a website's bulletin board, thus allowing the website owner to claim immunity under § 230.[94]

The court in the following case held that the publication requirement of § 230 was not satisfied. In *City of Chicago, Illinois v. StubHub!, Inc.*, the court rejected the defendant's argument that a city's amusement tax imposed on their website was the type of publication to which § 230 immunity applied.[95]

3. Third-Party Content

The courts in the following cases held that § 230 immunity applied because the online entity was being treated as publisher of third-party content. In *Gibson v. Craigslist, Inc.*, where an advertisement for a handgun was placed under the incorrect online classified service category by an unknown individual, the plaintiff sought to treat the merchant as a speaker of third-party content.[96] The court held the website operator was immune under § 230 and stated that this is the

USA, Inc., 29 Cal. Rptr. 3d 521, 544 n.9 (Ct. App. 2008).

92. *See* Miles v. Raycom Media, Inc., No. 09-CV-713(LG)(RHW), 2010 WL 3419438, at *2 (S.D. Miss. Aug. 26, 2010).

93. *Id.*

94. *See* Faegre & Benson, LLP v. Prudy, 367 F. Supp. 2d 1238, 1249 (D. Minn. 2005).

95. *See* City of Chicago v. StubHub!, Inc., 624 F.3d 363, 365-66 (7th Cir. 2010).

96. *See* Gibson v. Craigslist, Inc., No. 08-CV-7735(RMB), 2009 WL 1704355, at *3 (S.D.N.Y. June 15, 2009).

type of lawsuit § 230 was designed to immunize.[97] In *Doe v. MySpace, Inc.*, the court found that § 230 barred tort claims based on misrepresentation, when the claims sought to treat an ICS as a publisher or speaker of third-party content.[98] In *Barnes v. Yahoo!, Inc.*, the court found that unauthorized postings on a social networking website immunized the website owner, because the information in question was entirely provided by another information content provider.[99] In *Gentry v. eBay, Inc.*, the court concluded that an online auction website that misrepresented the safety of an item was immune under § 230, because the safety information was created by a third-party.[100] Finally, in *Doe II v. MySpace Inc.*, the court found that a tort action to treat a social networking website as a publisher was barred by § 230, because the profile in question was entirely created by a third-party.[101]

However, the court in the following case held that § 230 immunity did not apply because the content in question was not entirely created by a third-party. In *Anthony v. Yahoo! Inc.*, the court found that an e-dating service was not immune because the service's manner of presenting user profiles, not the profiles themselves, constituted fraud, therefore, the service provider was not immune under § 230.[102] It is important to note that when a service provider publishes tortious content created solely by the ISP, this conduct falls outside § 230 immunity.[103] In *Anthony,* the court found that the dating service in question created false profiles to induce members to maintain memberships with the dating website.[104]

97. *See id.*, at *3-4.

98. *See* Doe v. MySpace, Inc., 528 F.3d 413, 419-20 (5th Cir. 2008).

99. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101 (9th Cir. 2009) .

100. *See* Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 711 (Ct. App. 2002).

101. *See* Doe II v. MySpace Inc., 175 Cal. App. 4th 561, 573-74 (Ct. App. 2009).

102. *See* Anthony v. Yahoo! Inc., 421 F. Supp. 2d. 1257, 1262-64 (N.D. Cal. 2006) (explaining that the e-dating website produced fictitious profiles, and thus the website operator became a content provider by creating profiles and § 230 immunity did not apply).

103. *See id.* (noting that when an ISP fully creates tortious content, immunity does not apply because the ISP turned into an ICP).

104. *See id.* (noting that the creation of false profiles was a marketing strategy implemented by the ISP).

The court clearly noted that immunity has not been extended when an ISP creates its own comments and other defamatory content, while accompanying third-party postings on its website.[105] Therefore, an important question to ask is whether an ISP turned into an ICP by exceeding its editorial prerogatives. If the answer is yes, then the ISP § 230 immunity will not apply.[106]

D. *The Emerging Trend of § 230*

The case law above has evolved around a broad application of immunity under § 230. However, recent case law has emerged which has limited the application of § 230 and a trend has developed.[107] The first prominent case in this emerging trend is *GW Equity LLC v. Xcentric Ventures LLC*.[108] In *GW Equity*, the court found that a website may lose immunity when it takes an active role in creating or developing the content at issue.[109] This type of heightened scrutiny of § 230 has been classified as "mixed use" analysis.[110] The second prominent case is *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*.[111] The court in *Roommates.com* found that a website operator may lose immunity when the operator "encourages" or "contributes" to the illegal content published on the website.[112] This type of heightened scrutiny has been classified as the "encouragement or solicitation of

105. *See* Hy Cite Corp. v. Badbusinessbureau.com, LLC, 418 F. Supp. 2d 1142, 1149 (D. Ariz. 2005).

106. *See* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 297-98 (D.N.H. 2008).

107. *See generally* Samuel J. Morley, *How Broad is Web Publisher Immunity Under § 230 of the Communications Decency Act of 1996*, 84 FLA. B.J. 8, 13 (Feb. 2010) (discussing the heightened scrutiny of § 230 immunity in current case law).

108. No. 07-CV-976-O, 2009 WL 62173, *1 (N.D. Tex. Jan. 9, 2009).

109. *See id.* at 18 (finding that the defendant provided a consumer complaint forum that included titles, headings, and editorial messages written by the website operator).

110. *See* Morley, *supra* note 107, at 14 (the new type of heightened scrutiny analysis applies when a website operator "significantly changes content to third party content").

111. 521 F.3d 1157 (9th Cir. 2008).

112. *See id.* at 1167.

illegal content analysis."[113] The third prominent case was *Chicago Lawyers' Committee v. Craigslist*.[114] The court in *Craigslist* did not mention the term immunity while applying § 230 and the court stated that§ 230 of the CDA "[c]annot be understood as a general prohibition of civil liability for website operators . . . ."[115] Additionally, the court explained that ISPs could be liable if the ISP "played a more direct 'causal' role in the creation of the information."[116] This has set the stage for what some legal analysts describe as an evolutionary trend in limiting § 230 immunity.[117]

VI. Analysis

The concept behind the Internet has been to facilitate unrestricted conversations between actors with little regulation or oversight.[118] Therefore, this environment is conditioned for deception, rumors, slander, and intentional misrepresentations involving real humans and imaginary humans.[119] In analyzing e-dating websites and immunity, the statutory scheme of § 230 must be plainly described.[120] Section 230 provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[121] Additionally, § 230 states that "[n]o provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access or availability

113. *See* Morley, *supra* note 107, at 14-15 (when a website owner requires a third party to submit or input information that "encourages" or "contributes" to illegal nature, immunity may not apply).

114. 519 F.3d 666 (7th Cir. 2008).

115. *Id.* at 669.

116. KrisAnn Norby-Jahner, Comment, *"Minor" Online Sexual Harassment and the CDA § 230 Defense: New Directions for Internet Service Provider Liability*, 32 HAMLINE L. REV. 207, 240 (2009).

117. *See* Morley, *supra* note 107, at 8, 13-16.

118. *See generally* Jay M. Zitter, Annotation, *Liability of Internet Service Provider for Internet or E-mail Defamation*, 84 A.L.R.5th 169 (2000).

119. *See generally* Jeffrey R. Elkin, *Cybersmears: Dealing with Defamation on the Net*, 9 BUS. L. TODAY 22, 23 (Jan./Feb. 2000).

120. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

121. 47 U.S.C. § 230(c)(1) (2006).

of material that the provider . . . considers to be . . . objectionable."[122]

With the legal framework established, the analysis of the emerging trend of § 230 immunity will proceed in Section A with a narrative analysis of the case law that defines the emerging trend. Following Section A, Section B will provide critical analysis regarding the emerging trend and argue that a narrower § 230 application is fully consistent with the policy and legislative findings of § 230.

A. *Narrative Analysis*

The immunity provision of § 230 has generally been interpreted by courts as a complete shield on lawsuits against websites for disseminating third-party content.[123] However, two recent cases have indicated that a previously limitless application of § 230 may be coming to an end.[124] Generally, the broad application of § 230 immunity has been based upon whether ISPs act as ICPs.[125] Some critics have noted that § 230 has been turned into a "blanket immunity" that allows websites to leave content online that is defamatory or invasive of privacy.[126] Thus, a trend in rethinking broad immunity has emerged.[127] The cases of *Roommates.com* and *Craigslist* outline that ISPs can also be ICPs at the same time, and a closer examination of the "creation" or "development" of the third-party content must be recognized.[128]

122. *Id.* § 230(c)(2).

123. *See* David L. Hudson Jr., *Taming the Gossipmongers*, 94 A.B.A. J. 19, 20 (2008); *see also* Morley, *supra* note 107, at 10 (finding that courts have been resistant to narrowing § 230 immunity).

124. *See* Hudson Jr., *supra* note 123, at 19.

125. *See* Morley, *supra* note 107, at 10.

126. Hudson Jr., *supra* note 123, at 19 (quoting professor of law Daniel Solove, George Washington University).

127. *See* Morley, *supra* note 107, at 10.

128. *See id.* at 14-15 (examining the importance of *Roommates.com* and *Craigslist* and the application of the ISP/ICP distinction).

1. The First Leading Case – *Roommates.com*

In *Roommates.com*, the court found that a website operator can be an ISP and ICP at the same time.[129] The court in *Roommates.com* drew a line of distinction between the two categories, and determined that if a website "passively displays" content created entirely by a third-party, then it is solely an ISP with respect to that content.[130] However, when a website "creates" the content or is responsible in "whole or in part" for the "development" of the objectionable information, then the website is also an ICP.[131] Thus, a website may be immune from liability by § 230 for some of its content, but liable for the content it helped create.[132] The court in *Roommates.com* noted that "Congress sought to immunize the removal of user-generated content, not the creation of [the] content" by passing § 230 of the CDA.[133] Thus, when an online user submits data on a profile page that is drawn directly from questions posted by an ISP, closer analysis of the objectionable information must be applied before granting § 230 immunity.[134]

Additionally, the court in *Roommates.com* noted that an ISP may become an ICP by aiding in the development of the objectionable content, concerning a user's profile.[135] In defining "development" the court in *Roommates* stated:

> [W]e interpret the term 'development' as referring not merely to augmenting the content generally, but to materially contributing to its alleged unlawfulness. In other words, a website helps to develop unlawful content, and thus falls within the exception of section 230, if it

129. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1171-72 (9th Cir. 2008) (holding that *Roommates.com* played a part in development of objectionable content).

130. *See id.* at 1162-63.

131. *See id.*

132. *See id.* at 1172 (holding defendant liable because it was an ICP for some of the objectionable content).

133. *Id.* at 1163.

134. *See id.* at 1172 n.32.

135. *Id.* at 1166 n.19.

> contributes materially to the alleged illegality of the conduct.[136]

It follows from this definition that a dating website who asks users to enter personal information (e.g., sex, race, religion) through drop down menus, and allows users to search profiles limited to those classifications, will retain immunity.[137] Additionally, it is important to understand that ISPs are complex entities, but when an ISP starts to participate in the development process, immunity must be scrutinized at a higher level.[138]

The court in *Roommates.com* noted that an ISP that allows users to add further comments to their profile is not "developing" the content.[139] Therefore, the message in *Roommates.com* is that if an ISP does not "encourage illegal content or design a process" that requires a user to enter illegal content, then the ISP will retain immunity.[140] For example, when an e-dating website provides questionnaires or hints on how to answer personal questions on a profile creation Internet page, the e-dating ISP will retain immunity as long as this content is fully provided by a third-party and is not illegal in nature.[141]

Furthermore, the court in *Roommates.com* clarified its analysis in *Carafano v. Metrospalsh.com, Inc.*, which concerned data e-dating websites collect from users in analyzing ISP/ICP liability.[142] The court analyzed a commercial Internet dating service within § 230, where an unknown person had used a computer in Berlin to create a dating profile without the knowledge or consent of the celebrity plaintiff.[143] The court found that a typical dating profile contains pictures, descriptive

136. *Id.* at 1167-68.

137. *See id.* at 1169 (finding that when an ISP asks users for legal profile information, that ISP does not turn into ICP).

138. *See id.* at 1170.

139. *See id.* at 1174-75 (ISPs retain immunity when a user adds whatever they want under the "additional comments" portion of profile).

140. *Id.* at 175.

141. *See id.* at 1166.

142. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121 (9th Cir. 2003).

143. *Id.* at 1121-22.

information like age and interests, and answers to various questions created by the Internet dating website to evoke a deeper personality connection between users for the reason of paying for the service.[144] In addition to the general profile data questions, the e-dating website involved in *Carafano* asked members to select multiple choice answers to additional optional questions, some of which were sexually suggestive.[145]

The court analogized an Internet's dating website profile classification system to that of an online auction website.[146] Accordingly, the court looked at *Gentry v. eBay, Inc.*,[147] in concluding that a highly structured "Feedback Forum" that categorized user feedback with a color-coded star system did not transform eBay into an ICP with respect to the representations of the products on the auctioneer's website, because eBay did not "create or develop" the underlying information of the products.[148] In a similar fashion, the court in *Carafano* noted that when an Internet dating website "classifies user characteristics into discrete categories and collects responses to specific essay questions, [it] does not transform" the website into an ICP.[149] The court in *Roommates.com* clarified their reasoning in *Carafano*, stating that the dating website at issue in *Carafano* was immune because the website operator did not contribute to the content's illegality, thus it was not held liable as an ICP.[150] Following this analysis, an important point in *Rommates.com* explained

144. *Id.* at 1121.

145. *Id.* (citing additional questions e-dating websites keep as optional to encourage sexually suggestive responses).

146. *See id.* at 1124-25.

147. 121 Cal. Rptr. 2d 703 (Ct. App. 2002).

148. *See Carafano*, 339 F.3d at 1124-25.

149. *See id.* at 1124.

150. *See* Fair Hous. Council of San Fernando Valley v. Roomates.com, LLC, 521 F.3d 1157, 1171-75 (9th Cir. 2003). The claim against the website was that it failed to review each user-created profile to ensure it was not defamatory. *See id.* This is the activity for which Congress established § 230, where the website operator was merely a passive conduit and thus could not be held liable for failing to detect and remove the false content. *See id.* In *Carafano*, the website operator had nothing to do with the user's decision to enter a false name and create a fictitious profile, whereas Roommates.com developed and enforced a system that subjected subscribers to discriminatory housing practices. *See id.*

that "[t]he mere fact that an interactive computer service 'classifies user characteristics . . . does not transform [it] into a 'developer' of the 'underlying information.'"[151]

The underlying factual differences between *Carafano* and *Roommates.com*, were that the dating website in *Carafano* did nothing to enhance the defamatory message—it did not encourage defamation, nor did it make defamation easier.[152] The dating website simply provided neutral tools designed to match-up romantic partners based upon their voluntary inputs.[153] In contrast, *Roommates.com* developed its website to force subscribers to divulge protected characteristics (protected by the Fair Housing Act) and discriminatory preferences, then matched-up potential roommates based upon criteria prohibited by the Fair Housing Act.[154] Thus, the court in *Roommates.com* found the ISP also acted as an ICP for some of the online content, therefore, § 230 immunity was not applicable to part of the objectionable data.[155]

2. The Second Leading Case – *Craigslist*

In *Craigslist*, the court found that the defendant-ISP, Craigslist, was not liable for discriminatory housing advertisements posted by third-party users.[156] However, the court made an important interpretation of § 230 by stating: "Subsection (c)(1) [of § 230] does not mention 'immunity' . . ." and that § 230 "as a whole cannot be understood as a general prohibition of civil liability for web-site operators and other online content hosts . . . ."[157] Additionally, the court highlighted that § 230 could bar a defense if an ISP plays a more direct causal role in the creation or development of the objectionable

151. *Id.* at 1172 (quoting *Carfano*, 339 F.3d at 1124).

152. *See id.* at 1171-74 (distinguishing facts in instant case from facts in *Carafano*).

153. *See id.*

154. *See id.* at 1167.

155. *See id.* at 1175.

156. *See* Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 672 (7th Cir. 2008).

157. *Id.* at 669.

content.[158] Accordingly, the court in *Craigslist* highlights how a narrower application of § 230 immunity may be applied to future cases as the line between direct causation and ISP creation becomes less distinguished.[159]

The court noted that § 230 is general and, when invoking a causation analysis, one must look at direct causation to objectionable content in determining if an ISP is also an ICP.[160] The court stated:

> Doubtless [C]raigslist plays a causal role in the sense that no one could post a discriminatory ad if craigslist did not offer a forum. That is not, however, a useful definition of cause. One might as well say that people who save money "cause" bank robbery, because if there were no banks there could be no bank robberies. An interactive computer service "causes" postings only in the sense of providing a place where people can post. Causation in a statute . . . must refer to causing a particular statement to be made, or perhaps the discriminatory content of a statement. That's the sense in which a non-publisher can cause a discriminatory ad, while one who causes the forbidden content may not be a publisher. Nothing in the service craigslist offers induces anyone to post any particular listing or express a preference for discrimination; for example, craigslist does not offer a lower price to people who include discriminatory statements in their postings.[161]

Finally, the court in *Craigslist* found that § 230 does not allow a party to "sue the messenger just because the message reveals a third party's plan to engage in unlawful

158. *See id.* at 671.

159. *See id.* at 671-72.

160. *See id.* (explaining that Craigslist played a casual role in allowing a third-party to post objectionable content, but that this was not the type of causation which § 230 bars from immunity).

161. *Id.* at 672.

discrimination".[162] Thus, the court noted that an ISP could fall outside of § 230 immunity if the ISP played a more direct casual role in the creation of the objectionable information.[163]

B. *Critical Analysis*

This Section will argue that the emerging trend of a narrower application of § 230 immunity is fully within the scope of the legislative purpose, findings, and policy of § 230.

During the creation of § 230, the drafters of the provision, Representatives Cox and Wyden, stated that their goal was "'relief . . . from the smut on the Internet'" and they intended to accomplish that goal by "'empower[ing] parents without Federal regulation . . .'" to keep smut away from our children.[164] "Representative Cox also stated that the Internet had 'grown up to be what it is without . . . help from the government.'"[165] Furthermore, as legal analysts note, the drafters of § 230 inserted the immunity provision to encourage ISPs to monitor and block "offensive" content when necessary.[166]

Following the passage of § 230 by Congress, courts began interpreting the provision expansively due to the findings and policy subsections of § 230.[167] The findings subsection highlighted that "'the Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.'"[168] Additionally, the policy subsection of § 230 established that the purpose of § 230 is "'to promote the continued development of the Internet'" and to "'preserve the vibrant and competitive free market that

162. *Id.*

163. *See id.* at 671-72.

164. *See* David Lukmire, *Can the Courts Tame the Communications Decency Act?: The Reverberations of* Zeran v. America Online, 66 N.Y.U. ANN. SURV. AM. L. 371, 372-79 (2010) (quoting 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Ron Wyden)).

165. Lukmire, *supra* note 164, at 380 (quoting 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Ron Wyden)).

166. *Id.* at 381.

167. *Id.* at 382.

168. *Id.* at 382 (quoting § 230(a)(4)).

presently exists for the Internet . . . ."'[169] Thus, courts have cited these finding and policy subsections of § 230 in applying broad immunity to ISPs.[170]

Although courts have used the finding and policy subsections in applying § 230 immunity broadly, those same findings and policy objectives can still be realized when limiting the scope of § 230 immunity.[171] When ISPs regulate in good faith, which was the purpose in creating § 230, a narrower-based immunity application still embodies this purpose by holding ISPs immune from liability when they choose to regulate. Accordingly, when ISPs do not act in a regulatory manner, but contribute to the creation or development of objectionable data, then the ISP may be considered "in whole or in part" an ICP.[172]

Therefore, the policy and finding subsections of § 230 are still realized, because the Internet will remain a free and unburdened market for ISPs as long as their activities do not involve creation or development of objectionable data.[173] Additionally, today, an ISP is more likely to function as an ICP concerning user profile data, registration contingencies, and pre-populated questions and answers.[174] This duality of ISP/ICP is apparent in the information digital age because a greater amount of data is being transmitted through ISPs, as ISPs are looking for more ways to generate revenue.[175] Thus, the emerging trend of a narrower application § 230 immunity will likely continue in the future, as the Internet expands and ISPs further develop into ICPs.[176]

One criticism of a narrower application of § 230 immunity is that online speech will be threatened and ISPs will undertake an unreasonable burden in determining what online

169. *Id.* at 382 (quoting § 230(b)).

170. *Id.* at 383-84.

171. *See generally* Norby-Jahner, *supra* note 116, at 250-51.

172. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008).

173. *See id.*

174. *See* Morley, *supra* note 107, at 8.

175. *See id.* at 14.

176. *See id.* at 14.

information is unlawful.[177] However, this concern is partly addressed by the "Good Samaritan" exception which allows ISPs to voluntarily self-regulate without fear that their actions will offend freedom of speech online.[178] Additionally, ISPs would not face any liability if the offensive data in question was provided by another ICP.[179] However, if an ISP is in part responsible for the creation or development of the data, then liability may arise.[180] The extent to this liability will vary, but the acknowledgment that liability may arise is narrowing the scope § 230.[181] Thus, the new trend of limiting § 230 immunity denotes a changing online environment where ISPs may be accountable for their actions if they in whole or in part helped in creating or developing the offending content.[182]

Another criticism of a narrower § 230 immunity is the disruption of the exercise of a publisher's traditional editorial functions regarding third-party information.[183] The logic behind such a broad application is that a narrower reading of § 230 would frustrate the main objectives of § 230 by discouraging ISPs from voluntarily regulating third-party data on their websites.[184] Critics claim that this would transform the Internet into an extremely sterile or highly polluted data medium, which is against the policies intended by § 230.[185] However, proponents for a narrower application note that when a website reposts a profile with slight modifications, it

177. *See* Lukmire, *supra* note 164, at 388-89 (describing proponents' argument for a broad application of § 230 immunity and the importance of keeping Internet traffic free from unreasonable interference from government).

178. *See* Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008).

179. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008) (holding that ISPs are completely protected under § 230 immunity if they remain an ISP and have not transformed into an ICP).

180. *Id.*

181. *See* Zeran v. Am. Online, 129 F.3d 327, 331 (4th Cir. 1997). *But see Craigslist*, 519 F.3d at 670 (finding that § 230 immunity is not as broad as applied in *Zeran* and noting that an ISP may also be an ICP).

182. See *Roommates.com*, 521 F.3d at 1162.

183. *See id.* at 1163.

184. *See id.* at 1175.

185. *See id.*

has generally been held that § 230 will provide immunity.[186] An important question courts have asked when interpreting a narrower § 230 immunity is whether a minor alteration to a profile rises to the level of development necessary for liability.[187] Thus, the answer to the question lies in applying a narrower application of immunity, by examining the amount of development the ISP engaged in and whether the ISP became part-ICP.[188]

Generally, courts have found that when a party initiating a claim against a website for tortious acts, the hurdle in getting over § 230 immunity is transforming the ISP into an ICP.[189] In *Craigslist*, the court explained that Craigslist could not be treated as speaker of a poster's content.[190] The court noted that in analyzing objectionable information, a court must keep in mind that "'information' is the stock in trade of ISPs" covering everything from "ads for housing . . . [to] biting comments about steroids in baseball . . ." and that ISPs will still be provided immunity under a stricter application of § 230 immunity.[191]

Additionally, causation regarding ISP liability requires a claim that a particular statement was made by the ISP or the discriminatory content of a statement was made by the ISP.[192] In that sense, a non-publisher can cause a discriminatory ad, while the forbidden content may be displayed by a publisher or a non-publisher.[193] For example, if Craigslist were to offer a lower price to people who made discriminatory statements, then Craigslist may be liable as part-ICP and part-ISP.[194] But, when an ISP is solely a messenger that reveals a third party's plan to engage in unlawful discrimination or conduct, then §

186. *See id.* at 1170.

187. *See id.* at 1175 (finding importance in asking how much alteration to third-party content was performed by ISP in order for liability to attach).

188. *See id.* at 1165.

189. *See id.* at 1162-63.

190. *See* Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 671 (7th Cir. 2008).

191. *See id.*

192. *See id.*

193. *See id.* at 671-72.

194. *Id.* at 672 (explaining example of Craigslist publishing illegal content, but in no way creating content, and thus did not turn into ICP).

230 provides immunity.[195]

VII. Conclusion

In summary, this Comment presented an emerging trend of limiting the application of § 230 immunity and argued that this emerging trend is within the purpose and policy set-forth by Congress in passing § 230. First, the background of traditional and Internet intermediaries was presented to establish a general framework of intermediaries. Second, a brief discussion of the Constitutional framework concerning traditional intermediaries was presented to acknowledge that those concepts, established by the U.S. Supreme Court, are still relevant today. Third, § 230's development, application, and discussion of the emerging trend in case law was presented to establish the conceptual and analytical framework in order to advance the emerging trend of a narrower application of § 230. Finally, the analysis of two defining cases representing the emerging trend were discussed, and the critical analysis of the emerging trend highlighted how a narrower application of § 230 is within the purpose and policy set-forth by Congress in enacting § 230.

In conclusion, today ISPs are limited in their ability to control the online environment they create or simply host.[196] Often, e-dating websites and social networking websites require members to verify certain information due to rising privacy and safety concerns.[197] An example of one social networking website that has strictly enforced its verification policy is Whyville.[198] Whyville requires children to pass a chat test and a license test before using the website.[199] Another

195. *See id.* at 671-72 (comparing phone companies and courier services to Craigslist as being a cause for discrimination in the sense that it was the messenger of discriminatory advertisements).

196. *See* Hudson Jr., *supra* note 123, at 19 (describing online environment as a gossip haven with no privacy).

197. *See* Norby-Jahner, *supra* note 116, at 260-62 (describing social networking websites taking proactive measures in ensuring user safety and content reliability).

198. *Id.* at 261.

199. *Id.* at 260-61 (describing some ISPs' taking active measures in user information safety, reliability, and legitimacy).

example is the dating website Match.com, which now verifies that its members are not registered sex offenders.[200] Thus, some ISPs have recognized a danger inherent on e-dating and social networking websites and have taken proactive measures.

Whether § 230 needs to be revised or read more narrowly is a disputed subject.[201] Many critics who oppose a narrow construction of § 230 claim that the Internet needs to remain a venue for the free exchange of all ideas.[202] However, the emerging trend of a narrower § 230 immunity suggests that ISPs are not going to be given unchecked powers.[203] The emerging trend of narrower § 230 immunity remains a controversial issue.[204] The terms "creation" and "development" in categorizing an ISP as an ICP will take on further meaning as courts analyze the evolving environment of Internet intermediaries.[205]

Accordingly, as the evolving analysis of ISP and ICP categorizations develop, many supporters of a "broad blanket" application of § 230 argue that doctrinal protections raise First Amendment issues.[206] But critics to this view note that the free-wheeling landscape of § 230 immunity needs to come to an end due to an increasing potential for abuse and fraud online.[207] Many courts have stated that § 230 was not intended to create a "lawless no man's land on the Internet"[208] nor is it a "general prohibition of civil liability for [ISPs and ICPs] . . . ."[209]

200. Eyder Peralta, *Dating Site Match.com Will Now Check Users Against Sex Offender Database*, NATIONAL PUBLIC RADIO NEWS (Apr. 18, 2011, 1:58 PM), http://www.npr.org/blogs/thetwo-way/2011/04/18/135514625/dating-site-match-com-will-now-check-users-against-sex-offender-database.

201. *See* Lukmire, *supra* note 164, at 410-11 (describing tension between advocates for broad and narrow § 230 immunity).

202. *See id.* at 404-10.

203. *See id.* at 406-10.

204. *See* Morley, *supra* note 107, at 13-16.

205. *See id.* at 14-15 (citing cases that limited § 230 immunity by analyzing whether ISP created, encouraged, or developed objectionable content, thus turning ISP into ICP).

206. *See id.* at 13 (finding supporters of broad § 230 immunity-based argument on constitutional rights).

207. *See id.* at 13-14.

208. *Id.* at 14 (quoting Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008)).

209. *Id.* at 14 (quoting Chi. Lawyers' Comm. for Civil Rights Under Law,

Therefore, the development of mixed use content analysis and encouragement of illegal use content analysis provides a glimpse of how § 230 might be applied in the coming decade.[210]

Today, as more data and information develops on the Internet, the issues of reliability, safety, and illegality concerning e-dating will advance the trend of a narrower § 230 immunity application.[211] Whether more fluid definitions of creation and development are applied or a strict categorical approach is adopted, the reach of § 230 seems to be taking a new turn in the ever-evolving Internet law landscape.[212]

Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008)).

210. *See id.* at 14-15 (finding supporting evidence through case law that new categories of limiting § 230 immunity is emerging).

211. *See supra* nn. 103-42 and accompanying text (describing shift of analysis to scrutinize ISPs who also conduct themselves as ICPs).

212. *See supra* nn. 103-47 and accompanying text (explaining new categories have emerged in analyzing whether § 230 immunity applies and applying heightened scrutiny to cases where ISP may also be ICP concerning objectionable information).