NEW TECHNOLOGY MERITS NEW INTERPRETATION: AN ANALYSIS OF THE BREADTH OF CDA SECTION 230 IMMUNITY

I. INTRODUCTION

In the current digital age in which electronic communication and electronic storage are growing at an exponential rate, social media and social networking websites have become a useful tool for users to keep abreast of current events, connect with friends and colleagues, and expedite the flow of information. Although these websites are extremely valuable tools of communication, they also present new legal concerns about user privacy, ownership and control of information, and protected speech.

This comment examines the current scope of immunity granted by Section 230 of the Communications Decency Act and argues for a re-examination and restriction of its breadth of immunity.[1] Part I details the provisions and interpretation of the Electronic Communications Privacy Act of 1986 and the Communications Decency Act of 1996 – the primary statutes enacted to protect electronic communication and promote Internet growth.[2] It summarizes prominent case law interpreting each provision, focusing on the court's broad interpretation of the Communications Decency Act based on the policy objectives of promoting Internet growth and encouraging websites to self-regulate their content.[3]

Part II continues on to analyze three rapidly developing areas in the Internet era and the law's ability to regulate them. As relatively nascent forms of technology, these three areas of focus – social media, user-generated advertisements, and data mining – were not directly contemplated by Congress in adopting the Electronic Communications Privacy Act and the Communications Decency Act.[4] In each of the three topic areas, the business perspective is analogized and distinguished from the consumer perspective, concluding with an assertion of the law's appropriate role in diffusing tension between the two viewpoints.

The first topic of analysis is social media and social networking sites. An overview of the various business trends and developments in social networking is provided, followed by related concerns from the public consumer standpoint. The second topic discusses user-generated advertisements, outlining

---

1. *See generally* Communications Decency Act of 1996 §509, 47 U.S.C. § 230 (1998) [hereinafter CDA].

2. *See generally* Electronic Communications Privacy Act of 1986 §§ 110(a), 201[a], 301(a), 18 U.S.C. §§ 2521, 2701-11, 3121-27 (2002); CDA, *supra* note 1.

3. *See* Zeran v. America Online, Inc., 129 F.3d 327, 334 (4th Cir. 1997); CDA, *supra* note 1, § 230(b)(1)-(3).

4. *See, e.g.*, Rebecca Tushnet, *Attention Must Be Paid: Commercial Speech, User-Generated Ads, and the Challenge of Regulation*, 58 BUFF. L. REV. 721, 733-40 (2010).

the potential benefits of this method of advertising as well as potential backlash. Finally, data mining technology as it exists is described along with its potential applicability and related concerns as applied to internet marketing and advertising.

For each topic of analysis, this comment analyzes the scope of immunity granted by the current interpretation of the Communications Decency Act and argues in favor of a revision in light of the increased types and amounts of information being posted on the Internet, as well as the variety of ways this information can be and is being used.[5] Social networking sites, user-generated advertisements, and data mining technology were not considered by Congress when drafting the Communications Decency Act.[6] Therefore, extending the grant of Communications Decency Act immunity to these new forms of technology does not necessarily align with the objectives the *Zeran* court sought to achieve with its broad interpretation.[7]

Seldom does an internet service provider or website operator actually introduce original content when operating a social networking website.[8] The essential business model of a social networking website sustains itself on user involvement and user content; however, it does not mean the content is left entirely untouched by the website operator.[9] Thus, instead of casting a wide net of immunity for any internet service provider that does not create or develop its own content, a more nuanced, factor-based test should be implemented. A totality of the circumstances approach to awarding Communications Decency Act immunity, with a fact-specific inquiry considering such factors as the type of claim being brought, the specifics of the posted content, what the internet service provider or website sought to achieve with the content, and the like, more effectively balance the policy goals of promoting internet usage with deterring illegal behavior.[10]

---

5. *See* CDA, *supra* note 1.

6. *See, e.g.*, Tushnet, *supra* note 4, at 740.

7. *See Zeran*, 129 F.3d at 332-34.

8. *See* Alfred C. Weaver & Benjamin B. Morrison, *Social Networking*, 41 COMPUTER 97, 97 (Feb. 2008).

9. *See id.*

10. *See* discussion *infra* Part III.

II. LEGISLATIVE BACKGROUND

A. *Electronic Communications Privacy Act of 1986*

The Electronic Communications Privacy Act of 1986 (ECPA) was enacted as a baseline level of protection for electronic information against unauthorized access or disclosure.[11] Title II – the Stored Communications Act (SCA) – is most relevant to the protection of electronic communications, including online postings, emails, and text messages.[12]

Congress was concerned about the potential for hacking and unauthorized access of electronic communication along with the facilities in which such technology was housed.[13] Thus, Congress enacted sections 2701 and 2702 of the SCA to specifically address these concerns.[14] The sections apply to providers of an "electronic communication service" defined as "provid[ing] to users thereof the ability to send or receive wire or electronic communications."[15] Section 2701 of the SCA makes unauthorized access or exceeding authorized access of a facility, where an electronic communication service is provided a punishable offense.[16] Section 2702 seeks to limit the potential for disclosure of customers' electronic communications or records.[17] The prohibitions of the section state "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[18]

---

11. 18 U.S.C. § 2511 (2006); Alexander Scolnik, *Protections for Electronic Communication: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 372 (2009).

12. Stored Communications Act of 1986 §201[a], 18 U.S.C. § 2701 (2002); Scolnik, *supra* note 11, at 375.

13. Scolnik, *supra* note 11, at 374-75.

14. 18 U.S.C. §§ 2701-02 (2008).

15. *Id.* §§ 2510(15), 2522.

16. *Id.* § 2701(a)(1)-(2). An offense committed for the purpose of "commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any. . .violation of the Constitution or laws of the United States or any State," is punishable by a fine or imprisonment, ranging from not more than 5 years to not more than 10 years, or both, depending on the number of offenses. *Id.* § 2701(b)(1). An offense committed in any other case is punishable by a fine or imprisonment, ranging from not more than 1 year to not more than 5 years, or both, depending on the number of offenses. *Id.* § 2701(b)(2).

17. *See id.* § 2702 (entitled Voluntary disclosure of customer communications or records).

18. *Id.* § 2702(a)(1).

B. *Interpretation of the Electronic Communications Act of 1986*

Based on the plain language of the statute, the term "electronic communication service" has been restrictively interpreted to include only a "service that provides users with [the] capacity to transmit electronic communications."[19] Thus, those companies, who provide products or services over the Internet, but do not provide the actual Internet access, are not considered "electronic communication service" providers.[20]

In re Jetblue Airways Corporation addresses the legality of transferring personal information from an airline's passenger database to a governmentally-contracted company for the purposes of improving national security.[21] The plaintiffs, a class composed of JetBlue passengers, allege defendants violated their privacy rights and the ECPA by unlawfully transferring their personal information to Torch, a data mining company.[22] The Department of Defense subcontracted with Torch to carry out an initial national security study, which required a national-level database of personal information.[23] With the assistance of the Department of Transportation and the Transportation Security Administration, Torch was able to obtain consent from JetBlue Airlines to share its passenger information.[24] The amassed data contained over five million electronically-stored passenger name records and was merged with additionally purchased data to include a wealth of personal information.[25]

Displeased by the sale and disclosure of their personal information, plaintiffs brought suit against JetBlue for an unauthorized disclosure against the terms of the ECPA.[26] The Eastern District of New York held the ECPA provisions did not apply to JetBlue Airways.[27] Although plaintiffs argued that

---

19. *In re* Jetblue Airways Corp., 379 F. Supp. 2d 299, 307; 18 U.S.C. § 2510(15).

20. *In re* Jetblue Airways Corp., 379 F. Supp. 2d at 307.

21. *Id.* at 304-05.

22. *Id.* at 305. Torch is a data mining company who proposed a scheme of "rigorous analysis of personal characteristics of persons" geared towards predicting which individuals pose a risk to national security. *Id.* at 304.

23. *Id.* at 304.

24. *In re* Jetblue Airways Corp., 379 F. Supp. 2d at 305.

25. *Id.* ("This data was merged. . .to create a single database of JetBlue passenger information including each passenger's name, address, gender, home ownership or rental status, economic status, social security number, occupation, and the number of adults and children in the passenger's family as well as the number of vehicles owned or leased.").

26. *Id.*

27. *Id.* at 310 (holding "JetBlue as a matter of law is not liable under § 2702 of the ECPA. Because the sole basis for the plaintiffs' ECPA claim against Torch is [a] . . .

JetBlue constituted an "electronic communication service" because customers transmitted their personal data through the JetBlue system to book flights, their argument overlooks a necessary distinction between a website operator and the provider of the electronic communication "service that allows such data to be transmitted over the Internet."[28] JetBlue can be distinguished from providers of an "electronic communication service" because they did not provide the actual technology that allowed its data to be transmitted over the Internet.[29] "Rather, JetBlue is more appropriately characterized as a provider of air travel services and a consumer of electronic communication services [.]"[30]

Although plaintiffs were unable to sustain an ECPA claim, the Eastern District of New York continued on to hold that there may have been a viable breach of contract claim.[31] JetBlue published a privacy policy, which "specifically represented that any financial and personal information collected by JetBlue would not be shared with third parties and would be protected by secure servers."[32] This privacy policy may be enough to constitute a contractual obligation between the airline company and its consumers.[33] If so, the Eastern District of New York concluded JetBlue may have breached its contractual obligation when it disclosed its passengers' personal information, without consent, and actual damages may be appropriate.[34]

C. *Communications Decency Act of 1996*

The Internet, as we are familiar with it today, began to take form in the late-1990s.[35] To promote their services and encourage user involvement, website operators began creating forums where users could connect with other users, post

---

conspiracy theory, the claim against those defendants cannot stand absent liability on the part of JetBlue.").

28. *See Id.* at 307; *see also* 18 U.S.C. § 2510(15).

29. *In re* Jetblue Airways Corp., 379 F. Supp. 2d at 307.

30. *Id.*

31. *Id.* at 317-18.

32. *Id.* at 304.

33. *Id.* at 316-18.

34. *In re* Jetblue Airways Corp., 379 F. Supp. 2d at 316-18 ("Resolution of this claim will require the Court to determine whether the privacy policy gave rise to a contractual obligation and, if so, what damages rules apply.").

35. *See generally* Barry M. Leiner et al., *A Brief History of the Internet,* INTERNET SOC'Y, http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf (discussing the commercialization of the Internet).

messages, and maintain networks.[36] This remarkable increase in the volume of information and content posted on the web presented issues of first impression for the court concerning what legal obligations website operators should carry.[37] Without much guidance for this new medium of communication, courts had conflicting views on how to adequately address claims against website operators for defamation.[38]

In *Cubby, Inc. v. CompuServe, Inc.*, CompuServe used information from third parties to post an electronic tabloid on its bulletin board.[39] The plaintiff sued CompuServe for libel for the statements contained in the posting.[40] Under traditional defamation doctrine, there is a distinction between the classifications of distributor and publisher.[41] In this case, the court classified CompuServe as a distributor, which shielded them from liability.[42] Because CompuServe did not review the content from third parties, nor did it know or should have known of the defamatory content, it was not found liable.[43]

However, in *Stratton Oakmont, Inc. v. Prodigy Services Company* (hereinafter "*Stratton*"), the court held Prodigy liable for defamation.[44] In *Stratton,* an investment banking firm sued a website for defamatory claims, which were posted on the website's electronic bulletin board.[45] Although these claims were similar to those presented in *Cubby*, because the website's policy maintained it had editorial control of the bulletin board's contents, the court held the website was a publisher and found it liable.[46]

---

36. *See generally* Danah M. Boyd & Nicole B. Ellison, *Social Networking Sites: Definition, History, and Scholarship*, 13 JOURNAL OF COMPUTER-MEDIATED COMMC'N 210, 214-15 (2007).

37. *See Zeran*, 129 F.3d at 328-35 (discussing liability of website operators for defamatory speech by third parties).

38. *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 141 (S.D.N.Y. 1991) (finding website operator not liable); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995) (finding website operator liable).

39. *See Cubby, Inc.*, 776 F. Supp. at 137.

40. *See id.* at 138.

41. *See id.* at 139. "'[T]he constitutional guarantees of the freedom of speech . . . stand in the way of imposing' strict liability on distributors for the contents of the reading materials they carry." *Id.* (quoting Smith v. California, 361 U.S. 147, 152-53 (1959)).

42. *See id.* at 139-41("[V]endors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation." (quoting Lerman v. Chuckleberry Publ'g, Inc., 521 F. Supp. 288, 235 (S.D.N.Y. 1981))).

43. *See id.* at 140.

44. *See Stratton Oakmont, Inc.*, 1995 WL 323710, at *5.

45. *See id.* at *1.

46. *See id.* at *4-5.

Recognizing the potential for a chilling effect on Internet growth, Congress quickly passed the Communications Decency Act (CDA) in 1996.[47] The CDA was passed as an integral portion of the Telecommunications Act of 1996.[48] The relevant section granting immunity is section 230, entitled "Protection for Private Blocking and Screening of Offensive Material."[49] When the CDA was enacted, the Internet was still in its formative years.[50] Thus, with its passage, Congress' primary goals focused on promoting growth of this technology unhindered by government regulation.[51] For policy reasons, based on the findings of Congress, the Internet was viewed as a potential gold mine for the spread of information and a flourishing, new industry.[52]

The statute distinguishes whether a party is classified as an "interactive computer service" or an "information content provider," and courts have awarded immunity based on the distinction.[53] According to the language of the statute, three conditions must be satisfied to acquire immunity.[54] First, immunity is available only to "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server . . . ."[55] Second, the liability must be based on the defendant's role as a publisher or speaker.[56] Lastly, immunity only extends to "information provided by another information content provider."[57] Fulfilling those three conditions precludes a defendant from liability.[58]

---

47. *See Zeran*, 129 F.3d at 331 ("Congress enacted § 230 to remove the disincentives to selfregulation created by the *Stratton Oakmont* decision.").

48. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

49. CDA, *supra* note 1.

50. See *id.* § 230(a)(1).

51. *See id.* § 230(b)(1)-(5) ("It is the policy of the United States to (1) to promote the continued development of the Internet . . . ; (2) to preserve the vibrant and competitive free market that presently exists for the Internet . . . ,unfettered by Federal or State regulation; (3) to encourage the development of technologies which maximize user control over what information is received by [those] who use the Internet . . . ; (4) to remove disincentives for the development and utilization of blocking and filtering technologies . . .; and (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking . . . .").

52. *See id.* § 230(a)(1)&(5) ("The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of education and informational resources to our citizens. . . . Increasingly Americans are relying on interactive media for a variety of political, education, cultural, and entertainment services.").

53. *Id.* § 230(f)(2)-(3); *Zeran*, 129 F.3d at 332-34.

54. *See* CDA, *supra* note 1, § 230(f)(2), (c)1.

55. *Id.* § 230(f)(2).

56. *Id.* § 230(c)(1).

57. *Id.*

58. *Id.* § 230(c)(1).

Congressional findings and policy objectives supporting the benefits of advancing Internet development justified the imposition of immunity from civil claims.[59]

In contrast, an "information content provider" is subject to liability.[60] As the original speaker or creator of the information, an "information content provider" can be held liable for defamation types of claims.[61]

D. *Interpretation of the CDA*

Zeran v. America Online was the first appellate case to interpret the CDA.[62] It is the seminal case in which the court adopted a broad interpretation of the immunity provisions of Section 230.[63]

The facts of this case state that an unidentified party posted a message on AOL's bulletin board advertising t-shirts with offensive messages related to the Oklahoma City bombing.[64] For those interested in purchasing the t-shirts, Zeran's phone number was listed as the contact.[65] As a result, Zeran received a high volume of calls with violent or threatening messages.[66] Zeran sued America Online, Inc. ("AOL") for the defamatory messages, unreasonable delay in removing those messages,

---

59. *Id.* § 230(a)-(b). "The Congress finds the following: (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent 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 Americas, with a minimum of government regulation. (5) Increasingly Americans are relying on interactive media for a variety of political, education, cultural, and entertainment services." *See, e.g., id.* § 230(a).

60. *Id.* § 230(f)(3) ("The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation and development of information provided through the Internet or any other interactive computer service.").

61. *See Id.*

62. Rachel Seaton, *All Claims are Not Created Equal: Challenging the Breadth of Immunity Granted by the Communications Decency Act*, 6 SETON HALL CIRCUIT REV. 355, 362 (2010).

63. *Id.* at 362-64.

64. *Id.* at 329 ("[A]n AOL bulletin board advertis[ed] 'Naughty Oklahoma T-Shirts.' The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City.").

65. *Id.*

66. *Id.* ("Zeran was receiving an abusive phone call approximately every two minutes.").

refusal to post retractions, and failing to screen for related postings afterwards.[67]

The Fourth Circuit held AOL, as an interactive computer service, was immune from liability for any claims based upon the postings by the third party.[68] The Fourth Circuit looked to the legislative intent behind the CDA and concluded that Congress wished to encourage internet service providers to self-regulate their sites' content.[69] The Internet was a relatively new technology, which had immense potential for growth.[70] Therefore, the court aligned itself with Congressional policy and did not wish to impose the breadth of tort liability onto internet service providers.[71] Considering the vast amount of content on the internet, subjecting internet service providers to liability for all content would incentivize providers to severely restrict the type and number of messages posted, thereby possibly infringing upon the First Amendment protections of speech.[72] If courts were to impose such liability onto internet service providers, the efforts to screen for potentially tortious material would increase the costs of operation such that internet service providers would no longer seek to do business.[73] This drastic hypothetical would run contrary to the policies the CDA was enacted to promote.[74]

Ultimately, *Zeran v. America Online, Inc.* greatly expanded the scope of immunity afforded by the CDA, concluding that the distinction between "distributor" and "publisher" was irrelevant.[75] The Fourth Circuit rejected the imposition of "distributor liability" as contrary to Congress' intent in the CDA.[76] The option to consider internet service providers as distributors had negative effects the court sought to avoid.[77] Because distributors would be subject to liability if they knew or

---

67. *Id.* at 328.

68. *Zeran*, 129 F.3d at 328.

69. *Id.* at 330-31; *see* CDA, *supra* note 1, § 230(b)(2).

70. *Id.* § 230(a)(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.").

71. *See Zeran*, 129 F.3d at 331 ("The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect.").

72. *See id.* at 333 (citing Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767, 777 (1986)).

73. *Id.*

74. *See* CDA, *supra* note 1, § 230(b).

75. *See Zeran*, 129 F.3d at 331-32.

76. *Id.* at 334 (stating "Congress has indeed spoken directly to the issue by employing the legally significant term 'publisher,' which has traditionally encompassed distributors and original publishers alike.").

77. *Id.* at 331.

had reason to know of defamatory content by a third party, service providers would be reluctant to investigate or screen material posted on their sites, thereby disrupting[78]the integrity of internet self-regulation, one of the main policy objectives of the CDA.[79]

The majority of early cases interpreting the CDA covered defamation-related claims of action.[80] The court received an opportunity to address CDA immunity applied to other claims of action in *Doe v. MySpace, Inc.*[81] Opting to expand the scope of CDA immunity even further, the Court broadened its interpretation of CDA immunity to include negligence claims.[82]

MySpace, Inc. is a social networking site, which allows members to create an online profile to serve as a "medium for personal expression."[83] The facts indicate that the plaintiff's daughter signed up for a MySpace profile claiming she was eighteen years old, when in reality she was only thirteen.[84] Thereafter, a nineteen year old male, Pete Solis, initiated online communications with her.[85] This eventually led to Julie giving out her personal telephone number to Solis, whom she later met up with.[86] During this visit, Solis sexually assaulted Julie.[87] The mother brought a negligence action on behalf of her daughter, Julie Doe, against MySpace, Inc. alleging the operator knew sexual predators were using their service to communicate with minors.[88] Additionally, plaintiff alleged the website's security measures and policies relating to age verification were ineffective.[89]

The plaintiff attempted to distinguish her case from precedent by focusing on a narrow interpretation of the CDA.[90]

---

78. *Id.* at 333.

79. CDA, *supra* note 1, § 230(b)(2).

80. *See generally* Carafano v. Metrosplash.com, 339 F.3d 1119, 1123-25 (9th Cir. 2003) (granting internet dating service statutory immunity from liability in tort); *Zeran*, 129 F.3d at 330-31 (holding CDA barred defamation claims against commercial interactive computer service provider); Prickett v. InfoUSA, Inc., 561 F. Supp. 2d. 646, 652 (E.D. Tex. 2006) (holding website owners immune from liability under CDA for listing plaintiffs names, addresses, and telephone numbers under "Entertainers-Adult" heading).

81. Doe v. MySpace, Inc., 528 F.3d 413, 415 (5th Cir. 2008).

82. *Id.* at 418.

83. *Id.* at 415.

84. *Id.* at 416 ("This action allowed her to circumvent all safety features of the Web site and resulted in her profile being made public. . .").

85. *Id.*

86. *MySpace, Inc.*, 528 F.3d at 416.

87. *Id.*

88. *Id.*

89. *Id.* at 421.

90. *Id.* at 419.

However, the court rejected this argument noting that nothing on the statute's face supports the plaintiff's narrow interpretation.[91] The Fifth Circuit further explained their broad interpretation of the CDA, stating that "[p]arties complaining that they were harmed by a Web site's publication of user-generated content have recourse; they may sue the third-party user who generated the content."[92] Effectively, the Court sought to promote the broad policy objectives behind the enactment of the CDA.[93]

Similarly, *Barnes v. Yahoo!, Inc.* dismissed a plaintiff's negligent undertaking claim against an internet service provider, alleging it negligently removed indecent profiles that had been posted by plaintiff's former boyfriend.[94] Under this claim, the company, Yahoo!, Inc., was treated as a "publisher" of the profiles and photographs, a theory barred by the CDA.[95] The website operator, which merely published the boyfriend's content, fit squarely into the definition of an "interactive computer service" to be granted immunity.[96]

In summary, the courts have cast a wide net of immunity with regard to the types of content and types of defendants covered.[97] The three broad elements that must be fulfilled for a defendant to qualify for CDA immunity are as follows: 1) defendant must fall within the definition of "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer service"; 2) liability must be based on being a publisher or speaker of the content; and 3) the content must have been "information provided by another information content provider."[98] Defendants ranging from internet service providers to real estate groups to social networking sites have been granted immunity for third party content posted on their websites.[99]

---

91. *MySpace, Inc.*, 528 F.3d at 418 ("Courts have construed the immunity provisions in § 230 broadly in all cases arising from the publication of user-generated content.").

92. *Id.* at 419.

93. *Zeran*, 129 F.3d at 330-31 ("Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injuries messages.").

94. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1109 (9th Cir. 2009).

95. *Id.* at 1104.

96. *Id.* at 1101.

97. *See id. See also Zeran*, 129 F.3d at 330-31.

98. CDA, *supra* note 1, § 230(c)(1),(f)(2) (1996).

99. *See e.g., Zeran*, 129 F.3d at 328; Shiamilli v. Real Estate Grp. Of N.Y., Inc., 952 N.E.2d 1011, 1014 (N.Y. 2011) (holding a blog dedicated to the New York real estate industry qualified for CDA immunity concerning claims related to an anonymous user's negative posts about a rival apartment rental and sales company); *MySpace, Inc.*, 528 F.3d at 414.

Additionally, any claim the plaintiff alleges, which derives from defendant's status or conduct as a publisher or speaker, precludes liability.[100] The adopted definition of publication spans "reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content."[101] The range of immunized claims are not limited to defamation but have been extended to necessarily include "any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online," including negligence, unfair competition, and the like.[102]

There have been a minority of websites and internet service providers that have not been afforded CDA immunity, usually where the defendant has taken affirmative steps to alter the original content or under a claim deriving from a breach of contract theory.[103] In *F.T.C. v. Accusearch Inc.*, the website operator was classified as an information content provider and therefore precluded from immunity under the CDA.[104] Accusearch Inc., was the owner of the Abika.com website which sold various types of personal data, including telephone records.[105] The Federal Trade Commission filed suit alleging Accusearch's sale of telephone records constituted an unfair practice.[106] However, Accusearch contended that they did not break any laws through their trade in telephone records and further countered that they were immune from any civil penalties under CDA protection.[107] In order to qualify for CDA immunity, a website must be considered an "interactive computer service," the claim must be based on the website's role as a publisher or speaker, and the content at issue must be created or developed by a third party.[108] The court resolved the immunity issue on the third ground.[109] To determine if Accusearch was the "information content provider" of the content at issue, the court entered into a two-prong inquiry as follows: 1) whether confidential telephone records are "developed" when sold to the

---

100. *Barnes*, 570 F.3d at 1102.

101. *Id.*

102. *Id.* (quoting Fair Hous. Council of San Fernando Valley v. Roommates.Com, L.L.C., 521 F.2d 1157, 1170-71 (9th Cir. 2008)).

103. *See* F.T.C. v. Accusearch, Inc., 570 F.3d 1187, 1189 (10th Cir. 2009); Cohen v. Facebook, Inc., 798 F. Supp. 2d 1090, 1093-97 (N.D. Cal. 2011); *Barnes*, 570 F.3d at 1097 (holding plaintiff's promissory estoppel claim was not barred).

104. *Accusearch, Inc.*, 570 F.3d at 1190-91.

105. *Id.* at 1190.

106. *Id.*

107. *Id.* at 1194-95.

108. *Id.* at 1196.

109. *Accusearch, Inc.*, 570 F.3d at 1197.

public over the Internet; and 2) if so, whether Accusearch was responsible for the development of the offensive content.[110]

To analyze the CDA's meaning of "develop," an analysis using the canons of statutory interpretation is appropriate.[111] In order to avoid superfluous statutory language, "develop" encompasses a broad meaning, extending beyond mirroring the definition of creation which is to "[m]ake something new" or "[c]ome into existence."[112] Rather, the definition of "develop" in the CDA, as construed by the courts, is "to make actually available or usable (something previously only potentially available or usable)."[113] Applying this definition to Abika.com, it is clear Accusearch made confidential telephone records available to the public, and thus, "developed" that data.[114]

For the second prong, the court analyzed whether Accusearch was "'responsible in whole or in part, for the . . . development' of the offending content."[115] Case precedent has concluded that "a service provider is 'responsible' for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content."[116] In this case, the offensiveness of the content is the publicly displayed telephone records.[117] Accusearch's actions were far from neutral conduct coincidentally leading to the publication of private telephone records.[118] Its actions were directly intended to promote the publication of private telephone information.[119]

In conclusion, Accusearch was appropriately considered an "information content provider," statutorily defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or

---

110. *Id.* at 1197–1201.

111. *Id.* at 1198.

112. *Id.* at 1197–98.

113. *Id.* at 1198; WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 618 (2002).

114. *Accusearch, Inc.*, 570 F.3d at 1198.

115. *Id.* at 1198 (quoting CDA, *supra* note 1, § 230(f)).

116. *Accusearch, Inc.*, 570 F.3d at 1199. Compare *Roommates.Com, L.L.C.*, 521 F.3d at 1174-75 (holding a roommate-matching service was liable for the development of discriminatory preferences because it prompted users to disclose their illicit preferences), *with* Carafano, 339 F.3d at 1123-25 (immunizing a dating website that only provided neutral tools, which users employed to create offensive content).

117. *Accusearch, Inc.*, 570 F.3d at 1199.

118. *Id.* at 1199–1201.

119. *Id.* at 1201 ("Accusearch solicited requests for confidential information protected by law, paid researchers to find it, knew that the researchers were likely to use improper methods, and charged customers who wished the information to be disclosed.").

any other interaction computer service."[120] Due to this classification, Accusearch was not absolved of liability for its sale of telephone records as an unfair trade practice.[121]

The 2011 District Court case, *Cohen v. Facebook, Inc.* asserts the potential for social network users to sustain on a misappropriation claim.[122] The prima facie elements for a common law misappropriation action do not require the defendant to be considered a publisher or speaker, and therefore, CDA immunity does not apply.[123]

Liability assessed under the breach of contract doctrine appears to be a more viable claim of action.[124] Under these situations, the website-defendant has undertaken some affirmative steps in its statements or policy terms to create a contractual obligation.[125] Even though the offending content may still originate from a separate information content provider, if the plaintiff has relied on the website's statements of nondisclosure, privacy, and the like, this may give rise to a potential breach of contract or promissory estoppel cause of action.[126] On its face, the route the courts have taken may seem contrary to the reasons for imposing CDA immunity in the first place.[127] However, upon closer inspection, it is apparent that holding a website-defendant liable, when it has adopted policies and terms expressly holding themselves out to their consumers, aligns with the CDA's goal of internet self-regulation.[128] The

120. *Id.*; CDA, *supra* note 1, § 230(f)(3).

121. *Accusearch, Inc.*, 570 F.3d at 1201.

122. *Cohen*, 798 F. Supp. 2d at 1093–97 (dismissing, with leave to amend, misappropriation claims solely because of the plaintiffs' failure to properly plead a resulting injury).

123. *Cohen*, 798 F. Supp. 2d at 1093–94. ("To state a claim for common law misappropriation, plaintiffs must allege '(1) the defendant's use of the plaintiff's identify; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercial or otherwise; (3) lack of consent; and (4) resulting injury.'" (quoting Newcombe v. Adolf Coors Co., 157 F.3d 686, 692 (9th Cir. 1998))). *See also* CDA, *supra* note 1, § 230(c)(1).

124. *See Barnes*, 570 F.3d at 1109; Bradley v. Google, Inc., No. C 06-05289 WHA, 2006 WL 3798134, at *4–5 (N.D. Cal. Dec. 22, 2006); *In re* JetBlue Airways Corp., 379 F. Supp. 2d at 324–27.

125. *Barnes*, 570 F.3d at 1099 (website's Director of Communications called plaintiff and stated she would "personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it."); *In re* JetBlue Airways Corp., 379 F. Supp. 2d at 304 (company's privacy policy stated "any financial and personal information collected by JetBlue would not be shared with third parties and would be protected by secure servers.").

126. *Barnes*, 570 F.3d at 1108 ("[O]nce a court concludes a promise is legally enforceable according to contract law, it has implicitly concluded that the promisor has manifestly intended that the court enforce his promise.").

127. CDA, *supra* note 1, § 230(b).

128. *Id.* ("Policy . . . to preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation.").

CDA can be interpreted as a baseline rule – immunity for speaking or publishing another information service provider's content.[129] However, liability can still be established when a defendant makes a promise, whether by contacting the plaintiff directly or including a clause in its privacy policy, "with the constructive intent that it be enforceable."[130] This is an implied agreement to alter the baseline and will not preclude a cause of action.[131]

III. ANALYSIS

Although the CDA has been unquestionably successful in shielding websites and internet service providers from liability in order to promote the growth of the internet, the statute should be re-examined to address the following major areas, which have experienced unprecedented growth in usage and information content in recent years.[132] This trend of exponential growth seems likely to continue in the upcoming years as well.[133] Relatedly, the law concerning social networking sites, user-generated advertisements, and data mining technology is still in its nascent form and raises issues that most likely were not considered or adequately addressed during Congress' fact-findings for the CDA.[134]

This section briefly describes the developing technologies of social media, user-generated advertisements, and data mining; addresses viewpoints from business and consumer perspectives, and discusses the role the law should have in each area. The legal analysis centers on how the CDA's current interpretation would apply to the new technology, the strengths and weaknesses of the current approach, and the benefits of a new totality of the circumstances test for immunity.

A. Social Media

Social media encompasses a variety of websites and applications, which connect users through "seemingly limitless

---

129. *Barnes*, 570 F.3d at 1100 (referencing section 230(c)(1) which states "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.").

130. *Barnes*, 570 F.3d at 1108.

131. *Id.* at 1108-09.

132. *See* discussion *supra* Parts II.C.-D.

133. Weaver, *supra* note 8, at 97.

134. *See generally* Rachel Seaton, *All Claims are Not Created Equal: Challenging the Breadth of Immunity Granted by the Communications Decency Act*, 6 SETON HALL CIRCUIT REV. 355, 357 (2010).

opportunities for communication and collaboration."[135] They are also referred to as social networking sites because their primary purpose is to create a social network between users, through the exchange of information and ideas.[136] Typically, social media websites require an entity to create a profile, either under a real name or by assuming an alias.[137] With a profile, the user can then publish original statements, re-link news articles, comment on other users' statements, and much more.[138] Popular examples of these social networking websites include Facebook, MySpace, Twitter, and LinkedIn.[139]

From a business perspective, social networking sites commonly have a high valuation due to low overhead costs and large aggregates of valuable user information.[140] Without any tangible product being produced, it is difficult to understand exactly how their high worth is being calculated. One theory is that the production of information is considered valuable, and society has historically sought to incentivize the production of information.[141] Information spawns knowledge, creativity, innovation, and can provide the spark necessary to boost industries.[142] Thus, information can be seen as a social networking site's main "product."[143] Unlike tangibles, such as songs and DVDs, which have low reproduction costs, social networking sites tap into previously inaccessible personal information and identifiable content.[144] As a company, social networking sites are able to capitalize on this wealth of knowledge.[145]

Each user of a social networking site volunteers an assortment of personal information by creating a user profile and

---

135. Weaver, *supra* note 8, at 97.

136. *Id.*

137. *See generally id.*

138. *See id.* ("A social-networking site typically allows users to post their profiles and create personal networks for exchanging information with other users.").

139. Lawrence Morales II, *Social Media Evidence: "What You Post or Tweet Can and Will Be Used Against You in A Court of Law"*, 60 THE ADVOC. (TEXAS) 32, 33 (2012).

140. INA O. MURCHU ET AL., ONLINE SOCIAL AND BUSINESS NETWORKING COMMUNITIES (2004).

141. Albrecht Enders et al., *The Long Tail of Social Networking. Revenue Models of Social Networking Sites*, 26 EUR. MGMT. J. 199, 200 (2008).

142. *Id.*

143. *Id.* at 200-02 (social networking sites grant users access to contacts they would not normally remain connected to under traditional technology which allows website providers to benefit from this new potential of networking).

144. *Id.* at 201.

145. *Id.* at 205-09 (general methods social networking sites can employ to increase revenue are advertisements, subscription fees, and/or transaction fees).

participating in the online community.[146] Data encompassing age, gender, political affiliation, location, and interests are housed in the websites' databases.[147] As a business operation, social networking websites may be tempted to sell this information to researchers or other interested third parties.[148] Market analysts, advertisers, or any other entity needing a nationwide database of identifying data could benefit from information.[149] Furthermore, because an increasing number of social networking sites have gone public[150] or have discussed becoming publicly traded,[151] questions of what exactly investors are investing in and how these companies will maintain profitability are becoming more pressing.[152] With corporate investors pressuring social networking sites to be successful in the traditional sense of tangible dollars and not just the value of information, what methods will social media elect to use to transform the wealth of information into monetary wealth?

Tensions between the goals of businesses and the concerns of consumers have erupted in recent years as social networking sites have come under fire for inadequate disclosure of terms of service and misappropriating user-generated content.[153] Although, there is established case law granting these websites immunity from defamation and negligence claims, this new generation of claims takes issue not only with the third-party content, but also with the manners in which the websites are using or disclosing that content.[154] Under a plain analysis of the CDA, given the courts' current interpretation, a social networking site would be largely shielded from liability for numerous claims resulting from its role as the speaker or

146. *See generally* Weaver, *supra* note 8, at 98-100 (discussing case studies of four prevalent social networking sites).

147. *See id.*

148. Enders et al., *supra* note 142, at 205.

149. *See id.*

150. *See* Todd Wasserman, *LinkedIn IPO Is Set for Thursday*, MASHABLE BUSINESS (May 16, 2011), http://mashable.com/2011/05/16/linkedin-ipo-3/; Shayndi Raice, *Facebook Sets Historic IPO,* WALL ST. J., Feb. 2, 2012, http://online.wsj.com/article/SB10001424052970204879004577110001424052970.html.

151. *See* Tom Taulli, *Twitter Quietly Building Toward a Loud IPO*, INVESTORPLACE (Sept. 19, 2011), http://www.investorplace.com/ipo-playbook/twitter-ipo-zynga-groupon-facebook-lnkd/.

152. *See generally* Enders et al., *supra* note 142, at 205–09 (discussing different revenue models and customer satisfaction in social networking sites).

153. *See Cohen*, 798 F.Supp.2d at 1092; *In re* Twitter, Inc., No. C–4316, 2011 W.L. 914034, at *3 (F.T.C. 2011).

154. *See In re Twitter*, 2011 WL 914034, at *6 (discussion in Part II.D).

publisher of an information-content-provider's statements.[155] Operating on a bottom-up model, social networking sites provide applications giving individual users the power to create and develop content.[156] These websites no longer create or develop content for consumers to access.[157] Under this production model, social networking sites can qualify as interactive computer services and be immunized from any offenses in the user-generated content.[158]

By adopting a totality of the circumstances approach to CDA immunity, social networking sites would not receive such a strong grant of immunity. Instead, a court could apply the following factors to determine whether a social networking site should be afforded immunity: 1) the type of claim being brought; 2) the specifics of the posted content; 3) any actions the internet service provider or website has taken; and, 4) the policy objectives of the CDA.[159]

Applying the facts of *Doe v. MySpace, Inc.* to this new test exemplifies the effects of the factor-based inquiry.[160] The plaintiff in *MySpace, Inc.* brought a negligence-based action for insufficient age-verification measures.[161] Doctrinal elements of a negligence claim require the website to breach a duty owed to plaintiff, which proximately caused her injury.[162] Although, MySpace did not owe any sort of duty to Julie Doe under the specific facts of this case, it is possible that, with a slight change in the facts, a duty could be imposed.[163] What if the social networking site charged a subscription or user fee, creating a business-consumer relationship? Secondly, the specifics of the content here—a falsified age and personal telephone number—are relatively innocuous.[164] At the other extreme of offensiveness, consider if the content at issue concerned child

---

155. *See MySpace, Inc.*, 528 F.3d at 418; Weaver, *supra* note 8, at 97.

156. Weaver, *supra* note 8, at 97 ("The production model has shifted so that individual users now create content that everyone can share.")

157. *See id.*

158. *Id.*; CDA, *supra* note 1, § 230(c)(1).

159. *See* Seaton, *supra* note 135, at 376–81 (proposing a new test expanding on the principles of *Fair Housing Council v. Roommate.com, L.L.C.*). The proposed test considers "... the nature of the Web site at issue, the underlying facts of the case, and the claims brought by the plaintiff[,]" as "[t]he best way to effectuate Congress's intent in passing the CDA ...." *Id.* at 358.

160. *MySpace, Inc.*, 528 F.3d at 415–18.

161. *Id.* at 416.

162. Sport Supply Group, Inc. v. Columbia Cas. Co., 335 F.3d 453, 466 (5th Cir. 2003) ("[T]he elements of a negligence claim are (1) a legal duty on the part of the defendant; (2) breach of that duty; and (3) damages proximately resulting from that breach.").

163. *MySpace, Inc.*, 528 F.3d at 418.

164. *See id.* at 416.

pornographic images or videos concerning involvement in crimes. Courts may be more willing to hold a social networking site liable for blatantly offensive content under policy rationale.[165] The third factor targets actions by the social networking site, which are considered to "develop" the content at issue or have created a quasi-contractual obligation.[166] An example of a quasi-contractual obligation would be a provision similar to JetBlue's privacy policy promising the nondisclosure of information to third parties that could give rise to a claim of action for breach of contract.[167] The express statements of the Director of Communications, in *Barnes v. Yahoo!, Inc.*, may also qualify as a promise on behalf of defendant to end the unauthorized profiles of plaintiff.[168] Due to plaintiff's reliance on that promise, the defendant could be estopped from claiming immunity.[169] In *MySpace, Inc.*, it is questionable whether MySpace "developed" the offensive content.[170] In fact, MySpace's terms of use sway in favor of immunity by encouraging users to keep personal information private and not disclose personal information to new contacts over the Internet.[171] However, plaintiffs may make the argument that MySpace facilitated the creation of the public member profiles through an online user questionnaire.[172] Furthermore, plaintiffs could argue that MySpace's search function, allowing users to search by age, gender, and geographic location, manipulated the information enough to qualify the website as developing the content.[173] The merits of this potential plaintiff's argument have not been addressed by the courts.[174]

Intuition would suggest that social networking sites would be vehemently opposed to this new test as it could open the gates to costly litigation. Courts faced with a factor-based inquiry

---

165. CDA, *supra* note 1, § 230(b)(5) ("It is the policy of the United States to ensure vigorous enforcement of Federal criminal laws and to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.").

166. *See Accusearch, Inc.*, 570 F.3d at 1198 (defining "develop" as "to make actually available or usable (something previously only potentially available or usable)").

167. *In re* JetBlue Airways Corp., 379 F. Supp. 2d at 304.

168. *Barnes*, 570 F.3d at 1099.

169. *See id.* at 1108.

170. *See MySpace, Inc.*, 528 F.3d at 420-22.

171. *Id.* at 416 ("All members are cautioned regarding the type of information they release to other users on the Web site, including a specific prohibition against posting personal information such as telephone numbers, street addresses, last names, or e-mail addresses.").

172. *Id.* at 420.

173. *See id.*

174. *Id.* at 422 (Plaintiffs were barred from "argu[ing] that the CDA should not apply to MySpace because it was partially responsible for creating information exchanged between Julie and Solis" on appeal because it was not argued at the lower court level.).

often hand down decisions all over the map.[175] Thus, due to uncertainty and fear of being accused of developing or encouraging discriminating or illegal behavior, social networking sites might slow their technological development and innovation, stifling the spread of intellectual discourse.[176] However, this factor-based inquiry could also promote better self-regulation amongst social networking sites by improved drafting and enforcement of Terms of Use Agreements and privacy policies.[177] Thus, a new test could benefit social networking sites hoping to gain a competitive advantage by opting to take a proactive approach. Formulating a clear business plan and privacy policies will mitigate the consumer's fear of invasion of privacy and protect the social networking company from costly litigation.

B. User-generated Advertisements

User-generated advertisements are content originally created by consumers or third parties and selected by advertisers or companies to promote their product.[178] An example is the popular short video showing an artistic display of fountains created by Mentos chemically reacting with bottles of Diet Coke.[179] Although neither the Mentos or Coca Cola companies initially sought or supported these videos, the videos were later welcomed by both companies as part of their advertising and marketing arsenal.[180] The ability for companies to easily adopt the original content of another provider raises some concerns with regard to false advertising claims and tort liability.[181]

Is the speaker of the advertisement the original, unaffiliated party or the advertiser-company itself? The distinction between the two is important because doctrinally an individual speaker is entitled to protected speech, and can, therefore, make false claims as long as they are not defamatory in nature.[182] On the contrary, traditional advertisers, such as corporate entities, are governed by the doctrine of commercial speech and can be held strictly liable for falsities.[183] Because traditional advertisers

---

175. *See generally Zeran*, 129 F.3d at 333-34.

176. *See id.* at 330.

177. *See* CDA, *supra* note 1, § 230(b)(2).

178. *See* Tushnet, *supra* note 4, at 738.

179. *Id.*

180. *Id.*

181. *Id.* at 742-43.

182. *Id.* at 738 ("[I]ndividual speakers can generally make false claims about products, as long as they are not defamatory and do not otherwise present a clear and present danger of harm.").

183. *Id.*

must research and substantiate any material claims they make, adopting an individual's piece of work, which is not stifled by as many regulatory concerns, for advertising purposes would be an easier route.[184] It benefits the company's goals of generating new advertising material without all the background effort and market research typically required under traditional methods, while also giving the individual creator his or her 15 minutes of fame.[185]

However, this seemingly beneficial method of advertisers' adopting user-generated content is not without its own host of problems.[186] Although Congress did not contemplate the usage of others' content for advertising benefits, under the CDA's statutory language, the creator of the inadvertent advertisement would be considered a separate information content provider, and the advertisers would be an interactive computer service.[187] Thus, as a matter of statutory interpretation, websites would be immune from posting user-generated advertisements because they could simply be disseminating claims created by another party.[188] Under this framework, advertisers and websites would be incentivized to bypass commercial speech regulations by adopting promotional materials under the guise of someone else's creation.[189] If a consumer generates an advertisement which largely dramatizes or asserts false statements about a competitor, the advertisement is protected as non-commercial speech created by an individual expressing his or her First Amendment rights.[190] Without a showing of actual malice or defamation, the competitor would not be able to sustain a claim against the consumer.[191] Meanwhile, the manufacturer-advertiser, who posts the user-generated statements, would also be protected against legal action by a competitor because of immunity under the CDA.[192] Because the consumer is the actual information content provider, not the manufacturer-advertiser,

184. Tushnet, *supra* note 4, at 739, 743.

185. *See id.* at 743-44.

186. *See generally id.* at 740 (describing cases in which advertiser adoption of user-generated content triggered § 230).

187. *Id.* ("It's true that Congress didn't contemplate advertiser selection of others' content for commercial benefit. The model was AOL the web host, not AOL the advertiser holding a contest for the best user-generated ad for AOL services.").

188. *Id.* at 740.

189. *Id.* at 743.

190. Tushnet, *supra* note 4, at 742-43.

191. *Id.*

192. *See id.* at 740.

the insulted competitor may be left with no method of recourse at all.[193]

Although the policy behind the CDA's breadth of immunity has not changed, the potential for user-generated advertisements to "degrade (further) the integrity of information" disseminated requires an amendment to the CDA's immunity provisions.[194] In order to "promote the continued development of the Internet" and "preserve the vibrant and competitive free market," companies should not be incentivized to mask their promotional speech by explicitly adopting user-generated advertisements.[195]

These types of cases can be distinguished from the usual CDA immunity cases because an advertiser, who expressly adopts user-generated content, should be imputed with knowledge concerning the accuracy of adopted statements.[196] Unlike the typical social networking site or community forum that merely republishes statements users have provided without any affirmation of its validity, advertisers who adopt content to benefit their promotional and commercial endeavors are essentially certifying the user-generated statements.[197] Although the content may not have originated from the advertiser, it should not be immune from disseminating content that it knows or should have known are false.[198] Allowing advertisers to capitalize on this loophole runs contrary to the policy objectives of CDA immunity.[199]

C. Data Mining

Data mining is defined as turning a large collection of data into knowledge through data and pattern analysis techniques.[200] While data mining has not been specifically addressed by the courts in reference to internet content on social networking sites, cases have arisen concerning the propriety of data mining in the arenas of national defense and medical information.[201] The

193. *Id.* at 742-43.

194. *Id.* at 743-44.

195. CDA, *supra* note 1; Tushnet, *supra* note 4, at 743.

196. Tushnet, *supra* note 4, at 743-44.

197. *See id.* at 745.

198. *See id.*

199. CDA, *supra* note 1.

200. JIAWEI HAN ET AL., DATA MINING: CONCEPTS AND TECHNIQUES 2 (3rd ed. 2011).

201. *See, e.g.*, *In re* Jetblue Airways Corp., 379 F. Supp. 2d at 326-27 (holding that passengers' alleged loss of privacy as a result of airline's transfer of personal information to data mining company did not constitute damages available in a breach of contract action); *see also* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2668 (2011) (holding that the statutory burden on protected expression was not justified by State's asserted interests in

suggestion that it is only a matter of time before data mining technology is widely adopted in the social media world has been at the heart of concern surrounding Google, Inc.'s Googlebots.[202] Googlebots are computer programs which "crawl" around the Internet to track new content and update the Google index.[203] Recent news reports on the tracking capabilities of Googlebots foster a sense of uneasiness about the depth of information obtained via data mining and the permitted uses for this information.[204] As numerous social networking and internet startup companies elect to become publicly traded companies, the pressures of maintaining a profitable business model are increasingly important.[205] For example, companies may hire data mining companies or invest in their own data mining technology to collect pattern information about the demographics of those customers already using their services or persons generating traffic to the sites.[206] The companies can then refine their marketing strategies based on the analyzed data to target new consumers and retain current ones. The inherent concern amongst consumers and the general public is the potential for private information to be tracked and catalogued by the websites they are visiting from profiles they have created.[207] The illusion of having some veil of security combined with daunting language in privacy policies contributes to the consumer's increased sense of concern that "private" information may actually be available to the website company.[208] Although the courts have not addressed data mining in social networking sites,[209] a look at the issues of data mining, the court has touched on, may be instructive to future trends.

In 2011, the Supreme Court addressed the issue of data mining in the pharmaceutical sales industry in *Sorrell v. IMS*

---

patient confidentiality, protecting physicians from harassing sales behaviors, and protecting the doctor-patient relationship).

202. *Googlebot – Webmaster Tools*, GOOGLE.COM, http://support.google.com/webmasters/ bin/ answer.py?hl=en&answer=182072 (last visited Apr. 20, 2013) (describing how the Googlebot web crawling bot accesses sites every seconds to track content).

203. *Id.*

204. *See* Sarah J. Purewal, *Google Now Indexes Facebook Comments: Paranoid Can Relax*, PCWORLD (Nov. 2, 2011, 9:03 AM), http://www.pcworld.com/article/243011/google_now_indexes_facebook_comments_paranoid_can_relax.html.

205. *See, e.g.*, Enders et al., *supra* note 142, at 205-09.

206. *See id.*

207. Purewal, *supra* note 205.

208. *See id.*

209. *See* Silva Payne, *Explaining Data Mining*, HELIUM (August 23, 2009), Http://www.helium.com/items/1563301-data-mining-and-data-collection.

Health Inc.[210] In *Sorrell*, plaintiffs challenged Vermont's Confidentiality in Prescription law,[211] which prohibited the sale, disclosure, or use for marketing purposes of prescriber-identifying information without the prescriber's consent.[212] Because the statute "imposed content and speaker-based burdens on protected expression, is the Court subjected it to heightened judicial scrutiny."[213] Specifically, the statute disfavors marketing types of speech made by those in the industry on behalf of pharmaceutical manufacturers.[214] In order for this specific, content-based burden on protected expression to be constitutional under heightened judicial scrutiny, the State must show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to meet that interest.[215] The State argued that they have interests in lowering the costs of medical services, promoting public health, and keeping physicians' prescription decisions confidential.[216] While these may be valid interests, the Court does not address that issue because the statute does not advance the interests in a permissible way.[217] Because "the creation and dissemination of information are speech within the meaning of the First Amendment [,]" the "State may not burden the speech of others in order to tilt public debate in a preferred direction."[218]

This is the first case, which largely supports the idea of prescribing identification information as commercial free speech.[219] If corporate entities are given the same First Amendment protections to free speech as individuals are, how does this align with potential legal repercussions in the social networking and internet arena? Granting a corporation the right to free speech further immunizes the corporation against liability for third-party content. However, it is unlikely that Congress sought to immunize this huge breadth of speech and conduct

---

210. *Sorrell*, 131 S. Ct. at 2659.

211. VT. STAT. ANN. tit. 18, § 4631(d) (West 2009) (law held unconstitutional by *Sorrell v. IMS Health Inc.*).

212. *Sorrell*, 131 S. Ct. at 2659-60.

213. *Id.at 2663-64.*

214. *Id.* at 2663.

215. *Id.* at 2667-68

216. *Id.* at 2668, 2670.

217. *Id.* at 2658 (noting that "Vermont seeks to achieve those objectives through the indirect means of restraining certain speech by certain speakers. . . .But 'the fear that people would make bad decisions if given truthful information' cannot justify content-based burdens on speech" (quoting *Thompson v. Western States Med. Ctr.*, 535 U.S. 357, 274 (2002)).

218. *Sorrell*, 131 S. Ct. at 2667, 2671.

219. *See id.* at 2667.

when seeking to promote the proliferation of the Internet.[220] The CDA was enacted at a time when broad immunity for websites was necessary to encourage Internet growth.[221] Over recent years, an expansive breadth of immunity no longer seems necessary as the Internet is now flourishing as an established technology.[222] Furthermore, cutting-edge data mining technology no longer focuses on the individual pieces of content but on aggregates of information, changing the dynamic of potential claims that can be brought against websites.[223] The proposed factor test for CDA immunity allows for a more flexible approach to determine website liability by balancing the nature of the claims, content, actions taken by the website, and policy objectives of the CDA.

IV. CONCLUSION

Because of the broadly stated policy objectives of Section 230 of the CDA, the courts have pursued an equally expansive course of interpretation in granting internet service providers and websites immunity for third-party content.[224] In response, the Internet has grown rapidly over time, and the amount of websites and availability of information content on the Internet have increased exponentially. As a result, it is no longer imperative for courts to provide such robust protections of immunity.[225]

Conceptually, immunity is appropriate when a website merely republishes the content of a third party. However, often websites currently act as more than a neutral conduit for information to pass. Websites provide questionnaires and other tools to encourage user participation and the communication of information.[226] The companies operating these websites are developing commercial business models based on the wealth of their users' information, and it is appropriate to have a mechanism to hold them accountable, when necessary.[227]

---

220. *See, e.g.*, Tushnet, *supra* note 4, at 734-40.

221. *See* CDA, *supra* note 1, § 230 (1998).

222. Seaton, *supra* note 135, at 386-87.

223. HAN ET AL., *supra* note 201, at 3.

224. *See, e.g.*, *Zeran*, 129 F.3d at 335.

224. *Id.*

225. *See* Seaton, *supra* note 135, at 356-57.

226. Bill Tancer, *Hitwise US Research Note: Measuring Web 2.0 Consumer Participation*, HITWISE (June 2007), http://fastrackonlinemarketing.com/pdf/hitwise%20US%20-

227. *See Platform for Privacy Preferences*, SILICON PRESS (last visited April 20, 2013), http://www.silicon-press.com/briefs/brief.p3p/index.html.

A fact-specific inquiry would help ascertain the appropriateness of immunity. This approach would look at the totality of circumstances of a claim, considering the nature of the claims, specifics of the content, any actions taken by the website, and the policy objectives of the CDA. Although a factor-based test would make it more difficult to obtain immunity and fewer cases would be dismissed at the pleadings stage, this new method is better suited to address the entire spectrum of claims and websites. A factor-based test for CDA immunity will help foster policy objectives while also providing recourse for those parties legitimately harmed under the traditional doctrines of tort and breach of contract law. With the ascension of new areas of technology, the law should be able to react appropriately with a new method of interpretation.

Michelle Jee