UIC John Marshall Journal of Information Technology & Privacy Law

Volume 29
Issue 2 *Journal of Computer & Information Law - Winter 2012*

Article 3

Winter 2012

World Wide Web of Love, Lies, and Legislation: Why Online Dating Websites Should Screen Members, 29 J. Marshall J. Computer & Info. L. 251 (2012)

Maureen Horcher

COMMENT

WORLD WIDE WEB OF LOVE, LIES, AND LEGISLATION: WHY ONLINE DATING WEBSITES SHOULD SCREEN MEMBERS

MAUREEN HORCHER*

INTRODUCTION

Carole Markin met her "match" on Match.com ("Match").[1] Among the 1.3 million subscribers[2] looking for love on Match–20,000 singles joining daily[3]–the website filtered through the love-seeking throng and found a special someone for Carole. His name was Alan Wurtzel,[4] and he was hiding a dark, violent side. Of course Carole did not know that. She was simply signing online, hoping to meet another potential love connection. After all, the Internet has become one of the most popular places for lovers to meet;[5] love can truly be just a click away. As Carole prepared for her date with Alan, she had no idea that later that night, her "match"

* Maureen Horcher is a 2013 J.D. candidate at the John Marshall Law School in Chicago, Illinois. Maureen graduated magna cum laude in 2009 from Bradley Univeristy in Peoria, Illinois, with a degree in journalism. She would like to thank her parents, Bob and Michelle Hourcher, for modeling unapologetic faith and love. She would also like to thank Aaron Koonce, Laura Weiskopf, and Alana Yanagida for their unconditional friendship and guidance.

1. Cristen Conger, *Does Online Dating Work?*, ABC NEWS/TECHNOLOGY (Feb. 12, 2011), http://abcnews.go.com/technology/online-dating-work/story?id=12896317&page=2.

2. Nicholas Jackson, *Why Match.com Should Not Have Purchased Dating Website OkCupid*, THE ATLANTIC (Feb. 2, 2011, 10:59 AM), http://www.theatlantic.com/technology/archive/2011/02/why-matchcom-shouldnt-have-purchased-dating-site-okcupid/70651/.

3. Ki Mae Heussner, *Should Online Dating Sites Do Background Checks?*, ABC NEWS (July 10, 2010), http://abcnews.go.com/technology/online-dating-sites-background-checks/story?id=11063166.

4. Conger, *supra* note 1.

5. *Id.* (estimating that 23 percent of U.S. couples between 2007 to 2009 met online and stating, "[m]ore people meet online now than meet through school, work, church, bars, parties, et cetera.").

would brutally rape her in her apartment.[6]

Unbeknownst to Carole and the rest of the Match dating pool, Alan was a convicted sex offender.[7] In April 2011, Carole filed suit against Match, alleging that had Match screened its members, she would not have been raped.[8] Alan Wurtzel was not the only unobserved danger perusing Match. In November 2009, Ryan Logan, a thirty-four year-old Chicago man, was found guilty of raping a woman he met on Match earlier that year.[9] The website experienced further public relations embarrassment when it discovered the criminal history of another user, Abraham Fortune,[10] in a local newspaper.[11] His criminal status: convicted murderer.[12]

According to a Pew Research study, fifty-two percent of online daters said they do not find online dating dangerous.[13] More specifically, "users feel a certain comfort level that they won't run into sexual offenders or other criminals since they've paid for the service."[14] Despite that notion, Match openly opposed screening its members for criminal offenses. In July 2010, Match's general manager, Mandy Ginsberg, told ABC News that Match did not screen members because criminal and sex offender databases are occasionally inaccurate.[15] Screening would thus expose

---

6. Rachel Quigley, *Tired of Hiding: Match.com Victim Speaks out About Ordeal at the Hands of Convicted Sex Offender She Met on Dating Site*, MAIL ONLINE (Apr. 19, 2011, 9:38 PM), http://www.dailymail.co.uk/news/article-1378621/match-com-rape-victim-carole-markin-speaks-sex-offender.html.

7. Conger, *supra* note 1.

8. Quigley, *supra* note 6 (explaining, however, that Wurtzel was a misdemeanor felon. Even if Match.com had screened him using the federal criminal registry, his name would not have appeared anyway.).

9. Matthew Walberg, *Man Who Used Online Dating Site Convicted of Assault*, CHICAGO TRIBUNE (Nov. 9, 2010), http://articles.chicagotribune.com/2010-11-09/news/ct-met-match-com-rape-20101109_1_sexual-assault-judge-acquits-match-com.

10. Heussner, *supra* note 3.

11. *Id.*

12. *Id.*

13. *Online Dating: Summary of Findings*, PEW INTERNET & AMERICAN LIFE PROJECT (Mar. 5, 2006), http://www.pewinternet.org/reports/2006/online-dating/01-summary-of-findings.aspx (reporting that forty-three percent of online daters see risk in online dating; whereas, six percent of online daters think that dating websites do an "excellent" job of protecting users' information.).

14. Patrick Danner, *Love is Blind When Uninformed*, SAN ANTONIO EXPRESS-NEWS (June 24, 2010), http://www.mysanantonio.com/business/local/article/love-is-blind-when-uninformed-781503.php#ixzz1aCqbCL4y (reporting that "despite the fact that many online dating websites don't perform background checks, users feel a certain comfort level that they won't run into sexual offenders or other criminals since they've paid for the service").

15. Heussner, *supra* note 3 (reporting Match.com's General Manager Mandy Ginsberg's statement: "If we provide background checks, can they be accurate? And if they're not, do we give a false sense of security to people on the site . . . .That's the big concern I have. If someone slips through the cracks . . . does that create more of a risk for people to not be more prudent?").

users to greater safety risks because it would provide them a false sense of security.[16] Nonetheless, in an apparent effort to save face, Match retreated from that stance one year later. As part of Match's August 2011 settlement with Carole Markin, the website agreed to conduct criminal background screenings of its members.[17] In March 2012, Match, along with online dating providers eHarmony.com and Spark.com, publicly agreed to crosscheck subscribers against national sex registries.[18] The agreement is not legally binding or enforceable.[19]

While Match and others have backed down under public relations pressure, most dating websites refuse to treat user background checks as a prevailing trend.[20] Dating websites are not legally required to ask subscribers if they are convicted felons, screen members through a criminal database, or boot convicts from their websites.[21] Meanwhile, subscribers are paying their monthly registration fees, meeting people that the website matches them with, and unknowingly risking violent consequences.

This comment will explore the current immune-from-liability status of dating websites in subscribing felons and sex offenders to their websites. Additionally, this comment will explain why websites should screen for felons and sex offenders before matching paying users.

Section II will explore state proposed legislation requiring screening, which has generally been untried and/or unsuccessful.[22] Next, this section will detail current methods besides screening that dating websites implement to encourage safe dating practices. Section II will also examine the Communications Decency Act (CDA), the controlling federal legislation protecting websites from liability for allowing convicts to mingle and meet with their customers. This section will illustrate that the courts and Congress refuse to carve out exceptions to the CDA regarding user safety, and they claim legitimate policy reasons to do so. This sec-

16. *Id.*

17. Quigley, *supra* note 6.

18. Robert Jablon, *Three Online Dating Sites Agree to Screen for Predators*, USA TODAY (Mar. 21, 2012, 12:24 PM), http://www.usatoday.com/news/health/wellness/story/2012-03-21/Three-online-dating-sites-agree-to-screen-for-predators/53683868/1.

19. *Id.*

20. *IADW Opposes Background Check Legislation*, INTERNATIONAL ASSOCIATION OF DATING WEBSITES, http://www.iadw.org/14901.html (Sept. 26, 2011) (opposing screening for reasons such as a false sense of security and stating, "[a] woman could date a man thinking he has no criminal record because it was not uncovered by the background check, despite the fact that he was a murderer or rapist.").

21. Laura Hampson, *Site Singles Out Online Dating's Heartbreakers*, PALM BEACH POST (Jan. 7, 2011, 7:48 PM), http://www.palmbeachpost.com/money/site-singles-out-online-datings-heartbreakers-1170777.html (explaining that if users want to know the criminal history of their online dates, they must purchase software or hire investigators).

22. Martha L. Arias, *Are Online Dating Sites Regulated by Federal Law?*, INTERNATIONAL BUSINESS LAW SERVICES (Mar. 6, 2007), https://ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1684.

tion will explain that even if dating websites have knowledge of murderers and rapists on their websites, they need not remove them or warn other users of them.[23] Under current law, if one user murders another user on a first date, the dating website is exempt from liability, despite being essentially the proximate cause of that date.[24]

Section III endorses federal legislation mandating that fee-charging dating websites screen all subscribers, both upon initial registration and also on a specified periodic basis. This Section will recommend that the CDA policy not be the controlling force in dating website immunity because the status of Internet progress and security has dramatically changed since the CDA's inception in 1996.[25] The policies Congress used to secure the CDA fifteen years ago stand on shaky ground today. To balance the regulatory burden placed on the website provider, the proposal also precludes civil liability for dating websites that–despite proven good faith efforts to screen users–inadvertently register felons or sex offenders who later harm users. This would strike a balance between users' and website operators' competing interests and charge both parties with due diligence of safety.

In explaining this proposal, Section III will address both sides of the screening debate. This Section will explain the pro-regulation's safety argument as well as the anti-regulation's argument that online dating regulation would impose undue burdens on the websites, actually diminishing user safety.[26] Moreover, this Section will analyze whether an illegal invasion of privacy occurs when a website mandates a user to divulge his or her criminal history. In sum, Section III will demonstrate why the criminal screening argument is more persuasive than the no-screening argument. The public policy interests for screening are too immense for Congress to allow dating website operators to refuse protection of paying users by hiding behind CDA immunity. Finally, Section IV will conclude that screening legislation is likely inevitable; it is just a matter of *when* legislators will recognize the necessity.

BACKGROUND

Online dating is the third most popular way for singles to

23. Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (reasoning that, "notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services [and] any effort by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and therefore create a stronger basis for liability").

24. *Id.*

25. Ryan W. King, *Online Defamation: Bringing the Communications Decency Act of 1996 in Line With Sound Public Policy*, DUKE L. & TECH. REV. 24 (2003).

26. *Online Dating*, INTERNET ALLIANCE (Sept. 9, 2012), http://www.internetalliance.org/articles/online_dating.shtml.

meet–more popular than bars, clubs, and social events.[27] There are approximately fifteen hundred dating websites on the Internet.[28] Dating websites like Match, eHarmony.com ("eHarmony"), and Chemistry.com ("Chemistry") are open to anyone who subscribes and pays a monthly fee.[29] In addition to these traditional dating websites, the billion-dollar online dating industry[30] encompasses websites serving unique romance interests including: TrekPassions.com,[31] for StarTrek lovers; AshleyMadison.com,[32] for married people looking to have an affair; TallFriends.com,[33] for tall singles and those wishing to date them; and STDmatch.net,[34] for daters who share common STDs. Approximately twenty million Americans take advantage of these and other cyber matchmakers.[35] One in five relationships and one in six marriages are the result of online dating.[36]

Dating websites traditionally issue surveys to users, asking users to describe themselves and what they are looking for in a date or spouse.[37] The website matches users based on common characteristics such as location, hobbies, and religion.[38] The website may also allow users to assign different weight to characteristics and be matched accordingly. For instance, if a user values high income above hair color, then that website

27. Steven Barboza, *Digital Romance: The Business of Online Dating*, ATLANTA POST, 1 (May 3, 2011), http://atlantapost.com/2011/05/03/digital-romance-the-business-of-online-dating/ (reporting that the most popular way to meet is through workplace and school, and the second is through friends and family; reporting further that most users are part of the following online dating services: PlentyofFish, Zoosk, Manhunt, eHarmony, BeNaughty, OKCupid, ChristianMingle, TRUE, and Badoo).

28. *Id.*

29. Paul Farhi, *They Met Online, but Definitely Didn't Click*, THE WASHINGTON POST (May 13, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/12/AR2007051201350_pf.html (explaining why eHarmony.com rejects applicants).

30. Stefanie Rosenbloom, *New Online-Date Detectives Can Unmask Mr. or Ms. Wrong*, NEW YORK TIMES (Dec. 18, 2010), http://www.nytimes.com/2010/12/19/us/19date.html (explaining also that niche businesses have sprouted due to online dating and its associated dangers, which include businesses that conduct private background checks on people for a fee and even mobile phone apps) "Just plug in a couple of facts like a name and birth date. ValiMate, the creator of the Instant National Criminal Search app, even allows users to send the results of the check to a friend for added safety." *Id.*

31. TREK PASSIONS, http://www.trekpassions.com (last visited Sept. 7, 2012) (advertising free online dating for those interested in science fiction).

32. ASHLEY MADISON, http://www.ashleymadison.com (last visited Sept. 7, 2012) (advertising online dating for people already in a relationship).

33. TALL FRIENDS, http://www.tallfriends.com (last visited Sept. 25, 2011) (advertising as "the best and largest dating site for tall singles and tall admirers).

34. STDMATCH.NET, http://www.stdmatch.net/ (last visited Sept. 7, 2012).

35. Rosenbloom, *supra* note 30.

36. Barboza, *supra* note 27.

37. Ed Grabianowski, *How Online Dating Works*, HOWSTUFFWORKS (Sept. 9, 2012), http://people.howstuffworks.com/online-dating4.htm.

38. *Id.*

will focus on income before hair color in creating matches.[39] Some dating websites match users through multifaceted personality surveys and mathematical algorithms.[40] For example, eHarmony uses "twenty-nine key dimensions that help predict compatibility and the potential for relationship success."[41] These matchmaking formulas do not take into account a user's criminal history.[42] Crime bureaus have not yet begun recording crimes originating from online dating sources,[43] but violent stories like Carole Markin's are peppered throughout the news; more go unreported and unpublicized.[44] The next two sections will explore state attempts at online dating regulation and the current liability standing of dating websites to users who sue them.

The Regulatory Status Of Online Dating

The federal government does not regulate dating websites.[45] However, states such as California, Florida, Michigan, New York, Ohio, New Jersey, Virginia, and Texas have proposed or passed bills regulating dating website practices within their respective state boundaries.[46] Most of these bills or laws are similar to that of New Jersey's Internet Dating Safety Act ("Act"), the first legislation to regulate online dating.[47] In 2008, New Jersey legislature created the Act to facilitate public awareness of the possible risks associated with online dating activities. The Act states:

> An Internet dating service offering services to New Jersey members shall:
> A. Provide safety awareness notification that includes, at minimum, a list and description of safety measures reasonably designed to increase

39. *Id.*
40. *Id.*
41. *Id.*
42. Hampson, *supra* note 21.
43. Rosenbloom, *supra* note 30.
44. *Welcome to the Dangers of Internet Dating*, Dangers of Internet Dating, http://www.dangersofinternetdating.com/index.html (last visited Nov. 10, 2011) (stating "[t]he anonymity of internet dating has afforded con artists a new playground for scams, and has allowed people to be anyone they think you want them to be because they are engaging you primarily through the written word).
45. Arias, *supra* note 22 (noting, however, that some congressmen think there should be federal regulation) "For instance, Alan Cropsey, a Michigan State Senator said, 'It's like the wild, wild west out there." *Id.*
46. *Id.*
47. Gordon Basichis, *New Jersey Governor Signs First Online Dating Bill*, Hopeful Romantics (Jan. 15, 2008), http://www.hopefulromantics.org/2008/01/new-jersey-governor-signs-first-online-dating-bill/. "While the law, signed on January 14th, 2008, doesn't mandate background checks, it's a step in the right direction. This law will raise help awareness about the potential risks of online dating, which most users either don't know or don't want to know." *Id.*

> awareness of safer dating practices as determined by the service. Examples of such notifications include:
> (1) "Anyone who is able to commit identity theft can also falsify a dating profile."
> (2) "There is no substitute for acting with caution when communicating with any stranger who wants to meet you."
> (3) "Never include your last name, e-mail address, home address, phone number, place of work, or any other identifying information in your Internet profile or initial e-mail messages. Stop communicating with anyone who pressures you for personal or financial information or attempts in any way to trick you into revealing it."
> (4) "If you choose to have a face-to-face meeting with another member, always tell someone in your family or a friend where you are going and when you will return. Never agree to be picked up at your home. Always provide your own transportation to and from your date and meet in a public place with many people around."[48]

New Jersey law does not require dating websites serving New Jersey citizens to screen members, but it mandates that the website notify users whether or not it does so. According to the New Jersey Safety Act:

> If an Internet dating service conducts criminal background screenings, then the service shall disclose whether it has a policy allowing a member who has been identified as having a criminal conviction to have access to its service to communicate with any New Jersey member; shall state that criminal background screenings are not foolproof; that they may give members a false sense of security; that they are not a perfect safety solution; that criminals may circumvent even the most sophisticated search technology; that not all criminal records are public in all states and not all databases are up to date; that only publicly available convictions are included in the screening; and that screenings do not cover other types of convictions or arrests or any convictions from foreign countries.[49]

Despite honorable efforts of state legislators, dating websites can avoid such statutes by not advertising to citizens in those states.[50] Other providers that do not conduct criminal background checks still caution users of online dating risks through warnings listed within their terms of service policies. Despite Match's public promise to cross-check subscribers' names against public criminal databases, its terms of service explicitly warn that it does not currently conduct background checks.[51] At the same time, Match's terms grant the website authority to conduct criminal background checks at any time if it chooses.[52] The

48. Internet Dating Safety Act, 2007 N.J. Sess. Law Serv. 272 (West).

49. *Id.*

50. Arias, *supra* note 22.

51. *Match.com Terms of Use Agreement*, MATCH.COM (Sept. 7, 2011), http://www.match.com/registration/membagr.aspx?er=sessiontimeout.

52. *Id.*

website does not reveal what would trigger Match's operator to research a user's criminal history.[53] Moreover, Match explicitly denies all liability for injury resulting from use of their website.[54] Match states in its terms:

> [I]n no event shall Match.com be liable for any damages whatsoever, whether direct, indirect, general, special, compensatory, consequential . . . relating to the conduct of you or anyone else in connection with the use of the service, including without limitation, bodily injury, emotional distress, and/or any other damages resulting from communications or meetings with other registered users of this service or persons you meet through this service.[55]

While most dating websites weasel out of background checking, True.com, another dating website, screens every subscriber for felony and sex offense convictions,[56] without any legal obligation to do so.[57] Upon registration, users provide their full name and date of birth.[58] The website then checks that information against state and county databases for possible felony and sex offense convictions.[59] Since True.com's ("True") inception in 2003, the website has rejected approximately two to three percent of potential subscribers through the screening process.[60] "We turn away tens of thousands of felons [and] sex offenders . . . who, despite our warnings, try to communicate with our True members. At True, we take our members' safety seriously. We don't want felons [or] sex offenders . . . on our website, period."[61]

Unlike other dating websites, True does not bury safety information in its terms of service; such information is easily accessible from the homepage.[62] There it reads: "We can't guarantee criminals won't get on the Site, but we can guarantee they'll be sorry if they do."[63] Additionally, True's User Agreement reads: "I agree to adhere to the True Code of

---

53. *Id.*

54. *Id.* (clarifying that users are solely responsible for their actions with other members) "You understand that Match.com currently does not conduct criminal background checks on its members . . . Match.com also does not inquire into the backgrounds of all of its members or attempt to verify the statements of its members." *Id.*

55. *Id.*

56. Heussner, *supra* note 3.

57. TRUE, http://true.com (last visited Sept. 9, 2012).

58. *Safer Dating Guidelines*, TRUE (Sept. 9, 2012), http://www.true.com/magazine/saferdating_prosecute.htm.

59. Alissa Groeninger, *State Urged to Lower Risks of Online Dating: Legislation Would Require Sites to Disclose Whether They Do Background Checks on Clients*, CHICAGO TRIBUNE (Jan. 26, 2012), http://articles.chicagotribune.com/2012-01-26/news/ct-met-online-dating-regulation-20120126_1_dating-services-background-checks-site.

60. Heussner, *supra* note 3.

61. *Safer Dating Guidelines*, *supra* note 58.

62. TRUE, *supra* note 57.

63. *Id.*

Ethics and certify that: I have never been convicted of a felony or any criminal offense characterized as a sexual offense."[64] In the event that True discovers deceptive accounts, it can shut down that account, notify law enforcement, and/or pursue criminal and civil action.[65] True threatens prosecution of dishonest subscribers who are actually convicted felons by way of the Fraud by Wire, Radio, or Television federal statute,[66] which authorizes fines of up to $250,000 and up to five years in jail.[67]

The True model is an exception to the overwhelming non-screening trend. For, as it stands, choosing neither to screen nor to inform users about an inability to do so is completely legal–and quite possibly encouraged under the Communications Decency Act.

Communications Decency Act Immunizes Dating Websites From Liability

Section 230 of the 1996 federal Communications Decency Act[68] ("CDA") currently shields dating websites[69] from liability for matching convicted felons with unwitting subscribers.[70] The Good Samaritan clause states that, "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."[71] An Internet Service

64. *Safer Dating Guidelines*, *supra* note 58.

65. *Id.*

66. Fraud by Wire, Radio, or Television, 18 U.S.C.A. § 1343 (West 2008), reading the following:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

67. True, *supra* note 57.

68. Varty Defterderian, Note, *Fair Housing Council v. Roommates.com: A New Path for Section 230 Immunity*, 24 Berkeley Tech. L.J. 563, 565-67 (2009).

69. Doe v. Sexsearch.com, 502 F. Supp. 2d 719, 726 (N.D. Ohio 2007) (reading that "the CDA's immunity is not limited only to claims of defamation"). It has been applied to the Maryland Commercial Electronic Mail Act, a Florida securities law and cyber-stalking law, tortious interference and Title II of the Civil Rights Act of 1964.

70. *Zeran*, 129 F.3d at 333.

71. Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1996).

Provider (ISP)[72] is essentially any website provider. An information content provider is essentially a website or user providing substantive content to an ISP.[73] Courts use a three-part test to determine if an ISP enjoys CDA immunity: (1) whether the defendant provides an interactive computer service, (2) whether another content provider supplies the information regarding the postings at issue, and (3) whether the plaintiff seeks to treat the defendant as a publisher or speaker of third-party content.[74]

One of the pioneering cases in ISP immunity is *Zeran v. AOL*.[75] One week after the April 19, 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, an individual anonymously posted a message on an AOL virtual bulletin board advertising the sale of offensive t-shirts related to the bombing.[76] The post provided the plaintiff, Kenneth Zeran's, phone number for t-shirt inquiries and orders.[77] In fact, Mr. Zeran was not selling the offensive shirts and had no prior knowledge of this prank.[78] Angry calls flooded Zeran's phone line, which served both personal and business purposes.[79] Zeran argued that once he notified AOL of the defamatory content, AOL had a duty to remove the post in a timely manner, notify subscribers of the false post, and screen for future defamatory material, none of which AOL did.[80]

The Fourth Circuit disagreed with Zeran and held that Section 230(c)(1) of the CDA bars liability of an ISP exercising publishers' traditional editorial functions such as withdrawing, postponing, or altering content.[81] AOL was not liable for defamatory messages that users

72. Carafano v. Metrosplash.com, 339 F.3d 1119, 1123 (9th Cir. 2003) (defining an interactive computer service, also known as Internet service provider, as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer service, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or educational institutions").

73. *Id.* (defining an information content provider as "any person or entity that is responsible, in whole or in part, for the creation of development of information provided through the internet or any other interactive computer service").

74. Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 564 F. Supp. 2d 544, 548 (E.D. Va. 2008).

75. *Zeran*, 129 F.3d at 327.

76. *Id.* at 329

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.* at 333 (explaining that Zeran wanted to hold America Online liable for defamatory speech initiated by a third party).

81. *Zeran*, 129 F.3d at 330 (articulating that "by its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service; specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role").

posted on its virtual bulletin boards, notwithstanding a lengthy delay in removing the defamatory material.[82] The court said that the CDA protects ISPs who have knowledge of illegal material posted on their websites and still choose not to delete it.[83] The court also held that, pursuant to the Commerce Clause of the United States Constitution,[84] any state law that violates Section 230 is void.[85] In arriving at these conclusions the Fourth Circuit cited legislative policy written within the text of Section 230:

> It is the policy of the United States
> (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.[86]

In order to progress the fourth and fifth policy objectives concerning self-regulation and law enforcement, Congress added a second prong to the fifth policy, the Good Samaritan clause, of Section 230:

> 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

82. *Id.* at 327.

83. *Id.* at 333 "Notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any effort by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and therefore create a stronger basis for liability."

84. *Id.* at 334 (citing CDA language that "no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section").

85. Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977).

86. Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1996).

described in paragraph (1).[87]

Before Congress ratified CDA protection, an ISP's good faith effort to edit or remove material would have deemed it liable for that material's content.[88] ISPs would then naturally limit user activity on the website, thus discouraging free discourse among users.[89] In *Zeran*, the Fourth Circuit acknowledged that when Congress drafted the CDA, it recognized the threat that tort-based lawsuits present to freedom of speech.[90] Congress "considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect."[91] The court's holding in *Zeran* was that a plaintiff may only sue the user who wrote and/or posted false, misleading, or defamatory content, not the website displaying that content.[92]

The *Zeran* defamation case, which remains precedent for Section 230 ISP protection cases, was only the tip of the immunity iceberg. Since *Zeran*, courts have stretched ISP immunity to causes of action beyond defamation.[93] Courts attach immunity to operators of social networking websites, search engines, message boards, and shopping services.[94] Immunity also now touches the online dating realm.[95]

In the 1999 *Carafano* case,[96] an individual anonymously created a fake dating profile on Matchmaker.com ("Matchmaker") and posed as Christianne Carafano, a popular actress.[97] Carafano did not discover the sham profile until she began receiving sexually explicit messages and threats in response to her supposed profile.[98] Carafano sued the website for invasion of privacy, misappropriation of right of publicity, defamation, and negligence.[99] The Ninth Circuit held that even though Matchmaker posted the false information, the website did not create it and was therefore not liable for its falsity.[100] "Matchmaker cannot be

87. *Id.*

88. DiMeo v. Tucker MAX, 433 F. Supp. 3d 523, 529 (E.D. Pa. 2006) (providing an example of New York's holding that a service provider was liable because it screened and edited messages on its bulletin boards; therefore, it was subject to strict liability).

89. *Zeran*, 129 F.3d at 331.

90. *Id.*

91. *Id.*

92. Sarah Merritt, *Sex, Lies, and MySpace*, 18 ALB. J.J. SCI. & TECH. 593, 603-04 (2008).

93. *Carafano*, 339 F.3d at 1123.

94. Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008); Doe v. City of New York, 583 F. Supp. 2d 444, 449 (S.D.N.Y 2008); Parker v. Google, Inc., 422 F. Supp. 2d 492, 501 (E.D. Pa. 2006).

95. Defterderian, *supra* note 68, at 565-78.

96. *Carafano*, 339 F.3d at 1119.

97. *Id.* at 1121.

98. *Id.*

99. *Id.* at 1122.

100. *Id.* at 1124.

considered an 'information content provider' under the statute because no profile has any content until a user actively creates it."[101]

On the contrary, the court said that the website's matching services and e-mail notifications were precisely the type of continued Internet development Congress visualized when drafting Section 230.[102] The court plainly said that even though the questionnaire *elicited* information from individuals, the user *provided* the information, so liability remained on the user.[103] Matchmaker's act of collecting user responses and categorizing user characteristics "does not transform Matchmaker into a 'developer' of the 'underlying misinformation.'"[104]

In 2007, the Sixth Circuit affirmed the above ISP immunity holdings in *Doe v. SexSearch.com*.[105] "John Doe" joined SexSearch, a niche dating website for individuals seeking sexual encounters.[106] Doe scheduled a sexual encounter with "Jane Roe," age eighteen according to her profile.[107] It was not until police raided Doe's home and arrested him in December 2005 that he learned Roe's true age of fourteen.[108] Doe was charged with three separate counts of engaging in unlawful sexual conduct with a minor, which has a maximum sentence of fifteen years in prison and a permanent sex offender status.[109]

Doe sued SexSearch claiming the following: breach of contract, fraud, negligent infliction of emotional distress, negligent misrepresentation, breach of warranty, violation of the Ohio Consumer Sales Practices Act, and failure to warn.[110] SexSearch filed a motion to dismiss, claiming CDA immunity.[111] Doe responded that SexSearch reserved the right to modify profile content if it did not meet website guidelines, thus transforming SexSearch from service provider to content provider.[112] Therefore, Doe maintained preclusion of CDA immunity.[113] In granting SexSearch's motion to dismiss, the court held that, "while SexSearch

101. *Id.*

102. *Carafano*, 339 F.3d at 1123; *see also* Defterderian, *supra* note 68, at 565-78.

103. *Carafano*, 339 F.3d at 1124 (explaining that "the actual profile 'information' consisted of the particular options chosen and the additional essay answers provided. Matchmaker was not responsible, even in part, for associating certain multiple choice responses with a set of physical characteristics, a group of essay answers, and a photograph").

104. *Id.*

105. 105. Doe v. Sexsearch.com, 502 F. Supp. 2d 719, 726 (N.D. Ohio 2007), *aff'd*, 551 F.3d 412 (6th Cir. 2008).

106. *Id*.

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.* at 723.

111. *SexSearch.com*, 502 F. Supp. 2d at 724.

112. *Id*.

113. *Id.*

may have reserved the right to modify the content of profiles in general, Plaintiff does not allege SexSearch specifically modified Jane Roe's profile, and is thus not an information content provider in this case."[114] Furthermore, SexSearch's act of distributing, collecting, and posting a profile that Jane Roe answered falsely did not deem the website a developer of the content therein.[115] Once again, a judicial decision broadened the scope of ISP immunity.

Courts have also established that a plaintiff cannot allege liability by arguing that an ISP should have known that certain tools on the websites would advance illegal activity.[116] ISP action must go beyond sheer allowance and into intentional action.[117] An ISP may lose CDA immunity only "if it ceases acting as a mere passive conduit and takes an active role in creating, screening, and/or editing the unlawful content."[118] Such was the case in *Anthony v. Yahoo! Inc.*,[119] where the court precluded Section 230 ISP immunity for a dating website that allegedly created false profiles.[120] The CDA "clearly does not immunize a defendant from allegations that *it* created tortious content by itself, as the statute only grants immunity when the information that forms the basis for the state law claim has been provided by '*another* information content provider.'"[121]

In 2008, the Ninth Circuit held in *Fair Housing Council of San Fernando Valley v. Roommates.com* that a website that facilitates the development of unlawful content may lose Section 230 immunity if it "contributes materially to the alleged illegality of the conduct."[122] In that case, Roommates.com ("Roommates") matched individuals renting spare rooms with those seeking a place to live.[123] The court declared that Roommates' profile creation process violated Title II of the Civil Rights Act of 1964 by requiring subscribers to choose from pre-populated choices in answering questions regarding the user's sex, family status,

---

114. *Id.* at 725

115. *Id.* at 725-26.

116. Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1197-98 (N.D. Cal. 2009).

117. *Id.*

118. Richard B. Newman, *Online Defamation and the Communications Decency Act,* SITEPRONEWS (June 15, 2011), http://www.sitepronews.com/2011/06/15/online-defamation-and-the-communications-decency-act/ (noting that aside from certain narrow exceptions, "website operators are not liable for the content posted by its users").

119. Anthony v. Yahoo!, Inc., 421 F. Supp. 2d 1257 (N.D. Cal. 2006).

120. Newman, *supra* note 118 (noting that aside from certain narrow exceptions, "website operators are not liable for the content posted by its users").

121. Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1996).

122. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1168 (9th Cir. 2008).

123. *Id.* at 1161.

and sexual orientation.[124] The court said that in this instance, "Roommates becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information."[125]

The current law for ISP liability is clear. There is neither federal nor state law that mandates background screening.[126] Moreover, Section 230 forbids ISP liability in the case of an unscreened user's violent attack on another user, absent a website intentionally providing illegal content. This is because CDA public policy has nails dug deep in the judiciary, making reform impossible without specific legislation.

ANALYSIS

In 1996, Congress set the bright line immunity standard, which courts have since followed, citing Congressional intent, to grant immunity to ISPs.[127] As stated, Congress enacted Section 230 to encourage unfettered and unregulated development of free speech on the web, promote the development of e-commerce, and encourage ISPs and users of such services to self-police their websites.[128] However, as *Roommates* and *Yahoo!* illustrated, ISPs are sometimes liable when they actively elicit illegal material.[129] Exactly where ISP immunity ends and where liability begins is unsettled.[130]

True.com has pushed state governments to create legislation mandating that all online dating websites conduct background checks on their members or carry a disclaimer stating that they do not.[131] Criminal watch groups have praised the New Jersey legislature for answering that call.[132] "Millions of Americans look to online dating services every day as a quick, easy, and what they believe to be a safe way to meet new friends or find a partner," said Laura A. Ahearn, Executive Director of

---

124. *Id.* at 1166.

125. *Id.*

126. *Carafano*, 339 F.3d at 1124.

127. *SexSearch.com*, 502 F. Supp. 2d at 719.

128. Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1996).

129. *Roommates.Com*, 521 F.3d at 1157.

130. *Badging: Section 230 Immunity In A Web 2.0 World*, 123 HARV. L. REV. 981, 986 (2010).

131. Sarah Lacy, *Dinner, Movie, Background Check*, BUSINESS WEEK (May 9, 2005), http://www.businessweek.com/technology/content/may2005/tc2005059_8086_tc024.htm (noting also that the American Civil Liberties Union argues that background checks violate users' privacy).

132. *New Jersey Passes Bill to Make Online Dating Safer*, GOVERNMENT TECHNOLOGY (Jan. 15, 2008) http://www.govtech.com/security/New-Jersey-Passes-Bill-to-Make.html?topic=117671.

the Crime Victims Center.[133] "The Internet Dating Safety Act provides the one crucial element to minimize victimization–information. New Jersey lawmakers are to be commended for keeping our most vulnerable safe, and every state in the nation should follow their lead."[134] While True's push for state regulation is a beginning, state legislation is not a viable solution because adhering to fifty state laws would be too complex and cost-ineffective for dating websites to remain in business. Instead, the United States Congress must create cohesive legislation touching the four corners of the country.[135]

CDA Policy Has Grown Stale

The CDA essentially holds ISPs immune for the following activities: hosting third-party content, exercising traditional editorial functions, pre-screening objectionable content, paying third parties to submit content, and using drop-down forms or multiple choice questions if forms are legal.[136] These categories encompass broad activity and immunity serves a grave disservice to victims of violence perpetrated through the Internet.[137] The government should not grant near-blanket immunity to ISPs and website operators who do not screen people they are paid to match. The policies Congress stated in 1996 may have been pertinent–even necessary–then, but many of the policy concerns have since grown moot.[138]

The first congressional policy point supporting CDA immunity is the promotion of Internet development.[139] Since the CDA's inception, the Internet has grown exponentially. In 1996, thirty-six million people used the Internet, or roughly .9 percent of the world's population. Sixteen years later, 2.11 billion people use the Internet, 30.4 percent of the

133. *Id.*

134. *Id.* (noting also that many people think their online dating service conducts background screening) "This mistaken belief can have disastrous results. The new law gives consumers information they need to better make decisions on their safety." *Id.*.

135. *Online Dating*, *supra* note 26.

136. *Immunity for Online Publishers Under the Communications Decency Act*, Citizen Media Law Project (Sept. 9, 2012), http://www.citmedialaw.org/legal-guide/immunity-online-publishers-under-communications-decency-act (noting that, "[r]elatively few court decisions, however, have analyzed the scope of this immunity in the context of 'mixed content' that is created jointly by the operator of the interactive service and a third party through significant editing of content or the shaping of content by submission forms and drop-downs").

137. Matthew G. Jeweler, *The Communications Decency Act of 1996: Why Section 230 Is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers*, 8 PGH. J. Tech. L. & Pol'y 3 (2007).

138. Ryan W. King, *Online Defamation: Bringing the Communications Decency Act of 1996 in Line With Sound Public Policy*, 2003 Duke L. & Tech. Rev. 24 (2003).

139. Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1996).

world's population.[140] Congressional coddling of the Internet and ISPs is "no longer necessary because, far from fragile, they have become the dominant means through which commerce is conducted."[141] The Internet provides countless services that were unforeseen during Section 230's drafting, including interactive "services like YouTube, social networking services like Facebook and MySpace and graphically rich multiplayer games like World of Warcraft."[142] The Internet has grown so much that the CDA's rigid definitions of Internet Service Provider and Information Content Provider do not account for the parties' overlapping, collaborative content development.[143] Congress did not intend for the CDA to create this "lawless no-man's-land on the Internet."[144] Therefore, there should not be a general prohibition of ISP civil liability."[145]

The second congressional policy of encouraging a free market unfettered by federal or state regulation[146] is not only moot; it is irresponsible. Rather than supporting a cyber free-for-all, the government should curtail what *has* become that lawless, no-man's land,[147] as the Ninth Circuit described in *Roommates*. Dating website providers counter this conclusion saying that dating profiles are a form of speech, something the government always promotes.[148] Therefore, they argue that the second CDA policy has not grown stale and should remain untouched. Yale Law School Professor Jack Balkin argues accordingly:

> [Section 230] has had enormous consequences for securing the vibrant culture of freedom of expression we have on the Internet today. . . . Because online service providers are insulated from liability, they have built a wide range of different applications and services that allow people to speak to each other and make things together. Section 230 is by no means a perfect piece of legislation; it may be overprotective in some respects and under-protective in others. But it has been valuable

140. *Internet Growth Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/emarketing.htm (last visited Oct. 16, 2011) (noting that Marshall McLuhan's idea of a "global village" has become a reality).

141. *Roommates.com*, 521 F.3d at 1164.

142. T. Barton Carter, *Who is Safe in This Harbor? Rethinking Section 230 of the Communications Decency Act*, BOSTON UNIVERSITY FORUM ON PUBLIC POLICY 7 (2010), http://www.forumonpublicpolicy.com/archivespring08/carter.pdf.

143. Eric Weslander, *Murky "Development": How the Ninth Circuit Exposed Ambiguity Within the Communications Decency Act, and Why Internet Publishers Should Worry [Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008)]*, 48 WASHBURN L.J. 267, 292 (2008).

144. *Roommates.com*, 521 F.3d at 1164.

145. Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F. 3d 666, 669 (7th Cir. 2008); *see also* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003).

146. Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1996).

147. *Roommates.com*, 521 F.3d at 1164.

148. *Badging: Section 230 Immunity In A Web 2.0 World*, *supra* note 130, at 987.

nevertheless.[149]

The conclusion one must draw from Professor Balkin's view is that when Congress weighed free speech against public safety, free speech won.[150] Inserting that conclusion into the online dating issue, he might say that ex-felons and sex offenders enjoy free speech and thus should be able to surf dating websites notwithstanding past indiscretions. While free speech is undoubtedly a matter of great public interest and should be protected, Congress cannot ignore the resounding interest of safety.[151] "The short answer to the fear that potential liability for ISPs might chill or stunt online speech is that not all speech is supposed to go unregulated."[152] Preying upon others is an activity that *should* be chilled.[153] An unfettered Internet can be an unsafe Internet, and only Congress can safeguard its citizens from danger. Therefore, unfettered Internet activity is no longer sound CDA policy.

Criminal background screening does not necessarily upset Congress's third policy consideration–development of a user's control over what information he or she receives. Dating websites can still be innovative with user control while also screening for felons and sex offenders. Dating websites that choose to allow felons and sex offenders on their websites could place a warning on their profiles. This information would afford users greater control over what they send and receive. Thus, websites would actually increase user control because the user is more informed than if no screening took place.

The fourth congressional policy–to encourage ISPs to regulate themselves[154]–is an anomaly. The CDA authorizes ISPs to ignore illegal third-party activity on their websites. Congress, without any evidence, has simply "assumed that if it immunizes ISPs and website operators from liability, then those entities will screen content for defamatory material out of their own senses of altruism."[155]

In *Zeran*, the court said that Congress had established a "tacit *quid pro quo*" of offering interactive service providers broad immunity in exchange for their efforts to police themselves.[156] On the contrary, ISPs have *no incentive* to create blocking or filtration devices to protect their

149. *Id.*

150. Jeweler, *supra* note 137, at 3.

151. *Id.*

152. *Id.*

153. *Id.*

154. Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1996).

155. Jeweler, *supra* note 137, at 3.

156. Cecilia Ziniri, *The Optimal Liability System for Online Service Providers: How Zeran v. American Online Got it Right and Web 2.0 Proves it*, 23 BERKELEY TECH. L.J. 583, 587 (2008).

users.[157] To state this idea in practical terms, take for example the website, Vampersonals.com ("Vampersonals"), which is one of the largest vampire and gothic dating websites on the Internet.[158] Despite the fairly bizarre nature of this dating website, the federal government does not make the website screen its paying members.[159] The government assumes that Vampersonals on its own ensures that its vampire users will not sink fangs into each other's jugulars. Indeed, it is counterproductive to attempt to encourage these dating websites to self-regulate by immunizing them "regardless of whether the ISP attempts whatsoever to be responsible and screen its content."[160]

The final policy consideration–enforcement, punishment, and deterrence of law breaking–is contrary to the CDA's effects.[161] CDA immunity for dating websites precludes enforcement of laws and encourages ISPs to allow obscenity, violence, stalking, and harassment. Returning to the Vampersonals example, if one user viciously attacked another user with a stake on the first date, Vampersonals would not be liable under the CDA. The website would neither be responsible for enforcing laws and deterring crime, nor for the assault that, but for the website, would not have occurred.

In sum, the CDA should not be the end-all on possible ISP liability because its policy scope is too broadly construed. There must be *some* federal regulation on websites, and the CDA only works to refuse resolution for individuals harmed by online third-party content.[162] Even if Congress finds no cause to alter the CDA, it can create supplemental legislation to mandate screening without amending the CDA. Under Section 230, ISPs already enjoy editorial immunity, meaning that they can screen content prior to online upload without exposing themselves to civil liability.[163] The problem is that ISPs currently have no incentive to screen content. Whether ISPs screen users by ethical choice or by legal obligation would not change their editorially immune status under the CDA. The fact that the "website provider has policies and procedures or contract provisions to police its network does not lead to the conclusion that the website operator is responsible for the content created by the

157. Jeweler, *supra* note 137, at 3.

158. VAMPERSONALS, http://www.vampersonals.com/ (last visited Nov. 10, 2011) (touting itself as "one of the largest gothic and vampire dating sites on the net, a place where you can meet the vampire or goth (or both. . .!) of your dreams, as well as like-minded individuals in your area to spend time with, hang out, have fun and enjoy the darker sides of (un)life").

159. *Carafano*, 339 F.3d at 1124.

160. Jeweler, *supra* note 137, at 3.

161. Weslander, *supra* note 143, at 292.

162. *Id.*

163. *Zeran*, 129 F.3d at 330-31.

third party."[164]

Dating website legislation could mandate screening, and at the same time, align with Section 230 by not punishing ISPs for inadvertent screening inaccuracies. There are millions of online daters, and it would be unreasonable to expect dating websites to catch every criminal. However, the CDA currently protects websites that make no attempt to screen,[165] which should be offensive to all online daters. An inability to pledge flawless screening does not mean ISPs should be allowed to not screen at all. Considering the many CDA policies-gone-moot, Congress should plug the CDA gaps with safety regulation.

The Screening Debate

CDA immunity is only one part of the criminal screening debate. The other part asks if paid dating websites have an obligation to look for new ways to provide a safe environment for their users. If they have an obligation, should Congress determine what that obligation is and how it is fulfilled? Too much regulation will stifle the spirit of choice involving the online dating experience.[166] Moreover, ISPs might avoid creating dating web services for fear of liability stemming from user interaction.[167] Doing so would repress free speech and Internet growth–two consequences Congress intends to prevent.[168] The issue essentially breaks down into three elements: money, safety, and privacy.

The Internet Alliance, which represents dating websites in the fight against federal regulation, believes regulation of online dating service providers would impose unnecessary burdens on the industry and would not improve user safety.[169] Moreover, there are privacy implications when a website requires users to disclose personal information such as past crimes.[170] In sum, the Internet Alliance and other ISPs of similar mindset argue that it is enough for websites to display safety tips and investigate suspicious activity and complaints.[171]

---

164. Samuel J. Morley, *How Broad Is Web Publisher Immunity Under § 230 of the Communications Decency Act of 1996?*, 84 Fla. B.J. 8, 12 (2010).

165. *Id.*

166. *Zeran*, 129 F.3d at 331.

167. *Id.*

168. Ziniri, *supra* note 156, at 601.

169. *Online Dating*, *supra* note 26.

170. Tom Ahearn, *Online Dating Background Checks Fast and Easy But Not Always Accurate*, Employment Screening Resources (Feb. 14, 2011), http://www.esrcheck.com/wordpress/2011/02/14/online-dating-background-checks-fast-and-easy-but-not-always-accurate/.

171. *Online Dating*, *supra* note 26.

The Money Argument

Opponents of True's screening legislation proposal say that True is attempting to manipulate the online dating industry by destroying non-screening competition.[172] Additionally, the Internet Alliance says that legislation would unfairly target online businesses, forcing them to pay more than their offline counterparts.[173] Most offline dating outlets, such as newspaper singles advertisements and telephone-dating services, are unregulated and not required to screen.[174] The Internet Alliance argues that online dating websites should not be forced to invest time and money into screening just because their dating services are cyber, not print.[175]

The Internet Alliance further contends that tasking dating websites with criminal screening financially burdens them when users should investigate matches on their own.[176] The group says that background screening is too cost-ineffective to implement.[177] However, the Federal Bureau of Investigation provides free access to state sex offender databases.[178] Unlimited criminal background screening database software can cost as little as twenty-five dollars per month.[179] The Internet Alliance neither explains why such low cost is unduly burdensome, nor why that fee should be placed on already paying consumers rather than the moneymaking service. Moreover, if it would be easier for users to conduct their own screenings, then ISPs should display links to aid research. However, they do not, which is probably because they do not wish to draw attention to safety concerns.

Still, some dating websites consist of a single-digit staff and it would be virtually impossible to screen millions of users. Nevertheless, insufficient staff numbers is not a persuasive reason to ignore basic safety owed to a paying customer. These websites charge individuals a fee in exchange for a service. You get what you pay for–no fee, no screening. But users who invest their money into these websites expect more from a website than simple matching. After all, they could receive that same minimal service from free dating websites. Instead, they are entitled to

172. Donna Leinwand, *Background Checks Split Matchmaking Sites*, USA TODAY (Dec. 12, 2005, 10:39 PM), http://www.usatoday.com/tech/news/internetprivacy/2005-12-12-online-dating-checks_x.htm.

173. *Online Dating*, *supra* note 26.

174. *Id.*

175. *Id.*

176. *Id.*

177. *Id.*

178. *Sex Offender Registry Websites*, FEDERAL BUREAU OF INVESTIGATION, http://www.fbi.gov/scams-safety/registry (last visited Sept. 9, 2012).

179. *Unlimited People Search*, PEOPLE FINDERS, http://www.peoplefinders.com/checkout/offer.aspx?searchtype=membership (last visited Sept. 9, 2012).

an implied higher expectation, or at least a reasonable expectation that the service will not match its paid user with a murderer. If the website does not have enough money after advertising and registration profits to conduct cursory background checks, then it should change its business model, not forego user safety.

Matchmaking websites allocate time and money to conduct other types of screening. Criminal screening could be added to already existing screening procedures. For instance, eHarmony has rejected approximately one million people since its inception in 2000.[180] The dating website screens applicants and rejects them for various reasons, including if the applicant is separated but still married, if he or she is below twenty years of age, or if the person was married more than twice.[181] EHarmony also rejects applicants younger than sixty who have married more than four times and those who score low on traits such as emotional management, family background (happy childhood), and character.[182] Yet, the website does not screen for felons and sex offenders.[183] Why not add one more step in the screening process–likely the most important part of the online dating process? A user would probably care less if his match had been married than if she had murdered her ex-husband.

The Safety Argument

The Internet Alliance contends that the safety argument unfairly favors online dating versus offline dating outlets like singles advertisements.[184] The group argues that online dating is the same as meeting someone in a bar; only online dating is less risky.[185] The Internet Alliance argues that dating websites make the dating process safer because online profiles supply users with more information than offline dating

180. Farhi, *supra* note 29 (reporting Greg Waldorf, eHarmony's chief executive, as saying, "[w]e were founded with the mission to find happy, lasting relationships for people . . . It pains me that we're being put down or criticized for ensuring that we're doing the best job possible for our members").

181. *Your Question Answered: Why eHarmony Rejected You*, eHARMONY BLOG (Aug. 12, 2006, 2:05 AM), http://eharmony-blog.com/104 (explaining that there are sections in the test that ask: "if you have ill feelings in the last month, how you handle arguments, and how good your relationship is with your parents").

182. *Id.*

183. *Terms of Service*, eHARMONY (Sept. 9, 2012), http://www.eharmony.com/about/terms.

184. *Online Dating*, *supra* note 26 "Unregulated dating services are not a new phenomenon, running smoothly for years without legislative interference. Newspaper ads and single's hotlines are quite common and frequently used, providing even less information to interested parties about their potential date than is offered by a typical online profile."

185. *Online Dating*, *supra* note 26.

services.[186] Users can then evaluate the person's profile before talking on the phone or agreeing to meet.[187] The Internet Alliance further argues that a dating website that screens for felons and sex offenders would actually expose its users to increased vulnerability.[188] Public criminal databases are not always accurate.[189] Just because someone is not on a criminal database does not mean he or she has not committed a crime.[190] The Internet Alliance suggests that users are lulled into a false sense of security and will likely not conduct due diligence searches of their own.[191]

The Internet Alliance's argument is flawed. First, online dating *should* be safer than meeting someone in a bar because bars merely provide a place for customers to eat and drink; meeting potential dates is only a byproduct of that service.[192] Dating websites like Match not only provide a forum for users to mingle amongst themselves; their *primary service* is to *actively match* their users.[193] Moreover, if dating websites tout themselves as being safer because they reveal more information about prospects than meeting random people at bars, the websites should include *meaningful* information–something more than income level, physical characteristics, and a photograph.

Second, the anti-screening argument fails because it assumes that users do not currently hold a false sense of security and would only acquire one if the website began screening. Is it worse to have a false sense of security or no security at all? "I have dated other people on Match and I've had good experiences," Carole Markin of the Match lawsuit said.[194] "I just didn't expect that there would be somebody with a criminal background on the service. . . . When you've met nice, successful men previ-

186. *Id.*

187. *Id.*

188. *Id.* (arguing that the "Internet as a dating medium can arguably make the experience safer, as individuals have the opportunity to assess relationship potential well before a physical meeting occurs").

189. *Id.*

190. *Id.* (contending that "education and common sense, rather than unworkable laws and regulations, are the best way to protect consumers online").

191. *Online Dating*, *supra* note 26.

192. April Braswell, *Why Match Must Screen Singles Now*, APRIL BRASWELL BLOG (May 5, 2011), http://aprilbraswell.com/blog/whymatchmustscreen.htm ([c]ontending that dating websites "accept money from their clients to introduce people to each other. In which case, for that fee then I do think they need to perform a few basic background checks. To check prospective members against the sex crimes offenders registries seems like the basic level of background search to be performed").

193. *Id.*

194. Andrew Springer, *Woman Suing Match.com Over Alleged Assault Comes Forward*, ABC NEWS (Apr. 19, 2011), http://abcnews.go.com/us/woman-suing-match-alleged-assault-forward/story?id=13407806.

ously on the same site, you just don't assume the worst."[195] Carole Markin mistakenly assumed that Match protected her from rapists.[196]

Unfortunately, Carole Markin is not alone. Each year, Internet predators commit more than sixteen thousand abductions, one-hundred murders and thousands of rapes stemming from online services, including dating websites.[197] Yet, Internet dating advertisements focus on the success stories rather than the horror stories.[198] Consumers feed into that hype because "people WANT to believe they are going to find what they are looking for . . . and DON'T want to believe someone may be lying to them."[199] This perhaps naive expectancy escalates when the website charges for usage.[200] Users naturally assume there is a difference between paid and unpaid services, and the major difference should be security.[201] The Internet Alliance's argument also assumes without evidence that if websites screened applicants, users would be more reckless in their dating activities.

At the same time, the buyer must always beware and conduct personal investigations on his/her match. Many regulation opponents say that background checks are not sophisticated or accurate enough to mandate.[202] ISPs cannot possibly verify every applicant's detail for completeness and accuracy. The Internet inherently welcomes imposters, and there is no way to completely thwart deceit. Users must always take responsibility for their safety. Nonetheless, database blips do not deem screening a moot project. Laws are in place to deter, catch, and convict criminals, yet crimes still occur. Law enforcement does not stop seeking and punishing criminals just because crimes might still occur. New Jersey's legislature and others that have imposed online dating safety regulation have obviously put a high price on safety. But does safety trump privacy?

---

195. *Id.*

196. Braswell, *supra* note 192.

197. Tristan Watson, *Online Dating is Deceptive and Dangerous*, THE UNIVERSITY STAR (Apr. 14, 2009, 6:38 PM), http://star.txstate.edu/node/524 (arguing that traditional dating is safer than online dating) "Online dating is unsafe and can be deadly. Unfortunately, in our society people seek to harm others and one way to do this is through the Internet. Meeting people without the barrier of a computer will put structure back into the courtship process."*Id.*

198. *Welcome to the Dangers of Internet Dating*, *supra* note 44.

199. *Id.*

200. Braswell, *supra* note 192.

201. *Id.*

202. Leinwand, *supra* note 172 "Match.com spokeswoman Kristin Kelly says the rest of the industry is 'united against' background checks, in part because such checks often are incomplete and can give clients a false sense of security"

The Privacy Argument

Opponents of online dating regulation say dating website users should have the right to control what personal information they share, including felony incarcerations.[203] The argument goes that it is not the government's place to force them to disclose such private information.[204] "The notion that we should be requiring yet another industry to do background checks is chilling," said Barry Steinhart, director of the American Civil Liberties Union's Technology and Liberty Program.[205] "It hurtles us further into a surveillance society in which every action is going to be investigated."[206]

This argument can be quickly dispelled. Criminal convictions do not merit invasion of privacy claims because convictions are considered public records.[207] To have any interest in privacy, others must be excluded from obtaining the private information.[208] Moreover, this kind of disclosure is no different than what millions of private companies request on job applications. Most public and private companies require criminal background checks for jobs with children, the elderly, or disabled.[209]

In *Jensen v. State*, for instance, the Idaho Supreme Court held that requiring home-health service aides to disclose criminal backgrounds was not an intrusion on the aide's privacy (in that case, even requiring disclosure of expunged records).[210] There, the defendant did not actively breach the plaintiff's "private sphere or somehow actively uncover hidden facts."[211] Instead, the defendant asked the plaintiff to disclose such

203. Juliana Olsson, *Will Background Checks Reach Online Dating Sites?*, ROCKET LAWYER (Apr. 19, 2011), http://legallyeasy.rocketlawyer.com/will-background-checks-reach-online-dating-sites-9751.

204. David Colker, *Cupid Aims for Background Checks*, LOS ANGELES TIMES (Apr. 25, 2005), http://articles.latimes.com/2005/apr/25/business/fi-date25.

205. *Id.*

206. *Id.*

207. Elizabeth A. Gerlach, *The Background Check Balancing Act: Protecting Applicants with Criminal Convictions While Encouraging Criminal Background Checks in Hiring*, 8 U. PA. J. LAB. & EMP. L. 981, 999 (2006) (emphasizing that "if background checks are limited to revealing only convictions and not arrests that did not lead to convictions, the concern of privacy is greatly minimized").

208. United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000).

209. *Employment Background Checks: A Jobseeker's Guide*, PRIVACY RIGHTS CLEARING HOUSE (Sept. 9, 2012), https://www.privacyrights.org/fs/fs16-bck.htm (reporting that these background checks may include the following: driving records, vehicle registration, criminal records, social security number, education records, court records, bankruptcy, character references, medical records, property ownership, military records, drug test records, past employers, sex offender lists, incarceration records, and more).

210. Jensen v. State, 72 P.3d 897, 903 (Idaho 2003).

211. *Id.*

facts that could be discovered upon the defendant's research anyway.[212]

In the dating realm, the International Marriage Broker Regulation Act requires a U.S. citizen seeking a foreign fiancé to undergo a criminal background check before he or she can fly the fiancé to the United States.[213] Requiring background screenings for dating website subscription would move background screening requirements a minor step forward, helping to prevent violence and potentially saving lives.

In weighing the three main arguments of the screening debate–money, safety, and privacy–the answer is clear: dating websites must screen their users. Although paid websites have no legal duty to keep their users safe, such duty is implied. Users have a reasonable expectation that websites will attempt to preserve their safety. As long as online dating websites fail to screen their users, twenty million Americans are at the whim of these unregulated services.[214] The federal government must start proposing solutions.

A Possible Solution

In light of these overwhelming user safety concerns, Congress should draft federal legislation mandating that every fee-charging dating website conduct criminal background checks. The legislation should provide the following:

After an applicant registers on a dating website, the ISP shall run the name through public and/or private criminal and sex offender databases. Fee-charging dating websites shall prescreen their members and update profiles accordingly, every 365 days. If the website finds that an applicant has been convicted of a felony or sex offense, it has two options: 1) ban the offender from the website; or 2) notify users on the sex-offender/felon's profile page. The notification does not have to be obtrusive in size, shape, color, or font. Instead, the notification need only to be visible enough for a reasonable person to locate it on the page. Moreover, the notification need not state the name of the crime, convicting jurisdiction, or the date the crime occurred.

Further, a dating website shall retain business records of all felony and sex offender searches it runs. If the ISP can show it prescreened all members upon subscription and screened them every 365 days thereafter, users will be precluded from civil liability in cases of violence against

212. *Id.*

213. Holli B. Newsome, *Mail Dominance: A Critical Look at the International Marriage Broker Regulation Act and Its Sufficiency in Curtailing Mail-Order Bride Domestic Abuse*, 29 Campbell L. Rev. 291, 304 (2007) (reporting Congress created the International Marriage Broker Regulation Act of 2005 in response to two Washington mail-order bride murders. The Act requires "marriage brokers" to provide mail-order brides with information regarding violent criminal histories of marriage broker service users.).

214. Rosenbloom, *supra* note 30.

them. If the website conducted the search and a flaw occurred in the criminal database, then CDA Section 230 immunity will be upheld. If the ISP did not conduct any search, then immunity is precluded.

Take, for example, if this proposal was enacted and Carole Markin had sued Match. If Match could prove through records conducted in the course of business that it had criminally screened Alan Wurtzel, but did not find a sexual offense conviction, Match could assert a "pre-screening" affirmative defense and the case would be dismissed. If, on the other hand, Match had not conducted background searches, it would be exposed to liability. Simply stated, if the ISP cannot show that it attempted to keep users safe by conducting a two-minute background check, then immunity should not apply.

Though dating website operators may argue that this proposal is too strict, it actually offers middle-of-the-road regulation, balancing safety concerns with business cost concerns. Such legislation would still place buyer-beware onus on the user because he or she could not recover if the website conducted screenings. At the same time, this legislation merely injects slight regulation into an entirely unregulated arena. Through mandatory screening, ISPs would be forced to take responsibility–the kind of responsibility that the CDA currently impedes.

CONCLUSION

Like many online activities, online dating can be a valuable resource if used appropriately. While online dating websites bring people together that might not otherwise meet, the outcome is not always positive. For Carole Markin's sake, user safety must remain a primary concern.

The legislation proposed in this comment encourages ISPs to promote user safety by mandating that they expose dangerous subscribers. The CDA should not continuously shield ISPs because Congress did not intend for the CDA to license cyber anarchy.[215] ISPs cannot protest that safety regulation is inherently unfair and unduly burdensome. Dating websites are businesses. Like any other business, ISPs must stand behind their service–in this case, sparking romance between users. As Linda R. Greenstein, a proponent of New Jersey's Internet Dating Safety Act, states: "People who turn to the Internet to build new friendships and relationships deserve peace of mind that the person with whom they wish to form a connection is who they claim to be."[216]

---

215. Batzel v. Smith, 333 F.3d 1018, 1040 (9th Cir. 2003).

216. *New Jersey Passes Bill to Make Online Dating Safer*, *supra* note 132 (boasting that "the legislation arms consumers with valuable information by requiring Internet dating companies to disclose the extent of their safety measures, such as if they do or do not conduct background screenings on members who are seeking to date each other. . . doing so

ISPs may not be able to guarantee that a woman is every pound she claims to be, or that a man has every hair on his head that his picture portrays. They cannot guarantee against lousy dates, scams artists, or even violent attacks on their users. But the one thing all users should *always* be able to count on is that their dating service will not knowingly place them in harm's way. Websites like Match do not sweat over protecting their customers because they currently carry no liability. Congress *will* one day implement online dating regulation when safety concerns become too evident to ignore. The question remains: How many innocent people must be sacrificed before that time comes?

---

allows consumers to make more informed decisions regarding the online dating provider they choose to use").