ValpoScholar Valparaiso University Law Review

Volume 48
Number 1 *Fall 2013*

*pp.*329-368

Fall 2013

Rapists, Sexual Offenders, and Child Molesters: Who is Your Romantic "Match"? Why Dating Websites Should Perform Criminal Background Checks

Ryan D. O'Day

RAPISTS, SEXUAL OFFENDERS, AND CHILD MOLESTERS: WHO IS YOUR ROMANTIC "MATCH"? WHY DATING WEBSITES SHOULD PERFORM CRIMINAL BACKGROUND CHECKS

I. INTRODUCTION

Imagine a hardworking, career-driven woman named Sam.[1] Sam's busy life occupies her spare time, so she joins an online dating website in hopes of finding her significant other. After Sam spends endless hours creating a profile, the dating website recommends some possible dates based on Sam's answers. Eventually Sam encounters the profile of someone interesting, and the two decide to go on a date. On the night of her date, Sam expected to meet someone special; but, instead her date simply bides his time until he eventually sexually assaults and rapes Sam before leaving her in a dark alley.[2] Following this ordeal, Sam investigates her recommended date and discovers previous rape convictions. She wonders how the dating website recommended such a dangerous person. Although the prosecutor will hold Sam's date criminally responsible, the dating website could protect Sam from that harm; therefore, the law should allow Sam an opportunity to hold the dating website responsible for failing to protect her.

Dating websites can help prevent this situation by performing criminal background checks on users, but the websites will likely escape liability for failing to perform criminal background checks.[3] If states required dating websites to perform criminal background checks, situations like the one described may not occur, or in the alternative, if a website failed to perform criminal background checks, then it would face liability for its conduct.[4] However, without statutory guidelines, no duty requires dating websites to perform criminal background checks.[5] As a result, victims cannot hold dating websites accountable for failing to perform criminal background checks.[6]

---

1 This scenario is fictional and solely the work of the author.

2 *See infra* note 28 and accompanying text (listing criminal attacks on dating website users by their dates).

3 *See infra* Part II.C.1 (discussing the Communications Decency Act ("CDA"), and its grant of immunity to websites from tort actions).

4 *See infra* Part III.C.1 (analyzing how performing criminal background checks may affect dating website users online).

5 *See infra* Part III.B.2 (assessing that, without CDA immunity, current statutes do not impose a duty on online dating websites to perform criminal background checks).

6 *See infra* Part II.D.2 (discussing that the CDA immunizes online dating websites from a negligence cause of action).

This Note builds upon the proposals of other notes that recommended amendments to the Communications Decency Act ("CDA") and proposes that every state adopt legislation that requires online dating websites to perform criminal background checks and notify users of the results for their recommended dates.[7] First, Part II explains how online dating websites operate, provides an overview of current state statutes affecting online dating websites, discusses the history of the CDA and how the CDA grants immunity to websites from negligence causes of action, and considers the cost and effectiveness of criminal background checks.[8] Second, Part III analyzes the current safety procedures designed to protect dating website users, the CDA and its effect on website immunity, and the effects of requiring dating websites to perform criminal background checks.[9] Finally, Part IV proposes a model state statute that requires online dating websites to perform criminal background checks on users and notify users of their recommended date's criminal history.[10]

II. BACKGROUND

The popularity of online dating websites increased substantially in recent years, which increased the number of dates recommended by dating websites.[11] However, despite their popularity, no laws require dating websites to increase their security measures by performing criminal background checks before recommending a user as a potential date.[12] Part II.A gives an overview of the growth of online dating websites and the current requirements and risks involved with using an online dating website.[13] Part II.B lists state statutes affecting dating

---

7 *See infra* note 98 (discussing proposals of amendments to the CDA that would reduce the amount of immunity granted to websites from tort claims); *infra* Part IV (proposing a model state statute that would impose a legal duty on online dating websites to perform criminal background checks).

8 *See infra* Part II (providing an overview of online dating websites, statutes affecting dating websites, the CDA, common causes of actions brought by victims, and criminal background checks).

9 *See infra* Part III (analyzing current safety methods instituted to protect dating website users, the fairness of granting CDA immunity to websites, and whether criminal background checks will increase the safety of online dating and remain an economically feasible solution for dating websites).

10 *See infra* Part IV (proposing that each state pass legislation requiring that online dating websites perform criminal background checks on users).

11 *See infra* Part II.A (noting the growth of dating websites in recent years).

12 *See infra* Part II.B (listing statutes that affect dating websites and range from regulating user contracts to warning users about the lack of criminal background checks).

13 *See infra* Part II.A (discussing the popularity of online dating websites and the procedures and risks involved with using an online dating website).

websites and explains their impact on user contracts and the dating websites' security measures.[14] Part II.C explains section 230 of the CDA and the evolution of the Internet since the CDA's enactment.[15] Part II.D discusses tort liability by explaining common actions filed against online dating and social networking websites, and highlights CDA decisions granting immunity from negligence actions.[16] Last, Part II.E discusses the requirements, economics, and effectiveness of criminal background checks.[17]

A. Online Dating Websites

Industry leader Match.com launched its website in 1995 and helped turn online dating into a global service.[18] However, in the United States alone, approximately 1500 active dating websites serve millions of users.[19] The increase in popularity allowed the industry to double in size from 2007 to 2012 in both the number of people—twenty million in 2007 to forty million in 2012—and value—$900 million in 2007 to $1.9 billion in 2012.[20] Although some websites offer free basic memberships, the

---

14 *See infra* Part II.B (highlighting current state statutes affecting online dating websites).

15 *See infra* Part II.C (explaining the history of the CDA and the evolution of Internet use).

16 *See infra* Part II.D (listing the elements of common tort actions filed against social websites and explaining cases interpreting CDA immunity).

17 *See infra* Part II.E (explaining the use of criminal background checks to screen for dangerous individuals).

18 *About Us*, MATCH.COM, http://www.match.com/help/aboutus.aspx?lid=4 (last visited June 9, 2013). Match.com serves twenty-four countries and territories throughout the world in fifteen different languages. *Id.* Another popular dating website, eHarmony, started in 2000 and provides its services throughout the United States, Canada, Australia, and the United Kingdom. *Company Overview*, EHARMONY, http://www.eharmony.com/about/eharmony/ (last visited June 9, 2013). Although not popular in America, China's top dating website serves millions of users. *See Online Matchmaking Flourishes in China*, CHINA DAILY (Jan. 2, 2013), http://www.china.org.cn/china/2013-01/02/content_27565451.htm (discussing the large number of single young adults in China and how they turn to dating websites when under pressure by their parents to get married). Jiayuan.com, a popular Chinese dating website, serves over seventy-three million users and each day about seven thousand individuals change their relationship status to "in a relationship" or "married." *Id.*

19 Kristin Marino, *The Logic of Online Lovin': Does Online Dating Work?*, MBAPROGRAMS.ORG (Mar. 14, 2012), http://www.mbaprograms.org/news/does-online-dating-work.html. The highest number of visitors per month belong to ZOOSK with over fifty million in 2007, PlentyOfFish with thirty-two million in 2011, Match.com with twenty-nine million in 2012, and eHarmony with twenty million. *Id.*

20 *Id.* Online dating developed into a very profitable industry: IAC, owner of Match.com and its affiliate websites, reported revenues of $105.2 million in the fourth quarter of 2011, ZOOSK reported revenues over $90 million annually, and even niche dating services are cashing in as Spark Networks, owner of the niche service Christian Mingle, reported revenue of $12.7 million in the third quarter of 2011. *Id.* Although the

most popular sites—Match.com and eHarmony—charge fees ranging from $36 to $60 a month, respectively.[21] Many dating websites require users to complete a compatibility test allowing the site to recommend and match users based on answers to specific questions.[22] Dating websites may ask users to provide basic background information including: (1) age; (2) gender; (3) education; (4) profession; (5) family size; and (6) religion.[23] Some sites, such as eHarmony, may also ask users for more in-depth information including: (1) hobbies; (2) drinking

---

industry substantially expanded in recent years, four companies control 77% of the market. Anne VanderMey, *Outsourcing the Algorithm of Love to Online Dating*, CNNMONEY (Feb. 14, 2013, 7:02 AM), http://tech.fortune.cnn.com/2013/02/14/outsourcing-the-algorithm-of-love/. IAC, owner of Match.com and OkCupid.com, controls 41% of the market, eHarmony controls 23.5% of the market, Zoosk represents 7.7% of the market, and Spark Networks, owner of JDate, Christian Mingle, and many other niche websites, serves 4.9% of the market. *Id*. Additionally, new forms of revenue have developed as websites turn to mobile apps to increase revenue. Sharon Jayson, *Mobile Apps Tap the Changing Face of Online Dating*, USA TODAY (Feb. 13, 2013), http://www.usatoday.com/story/news/nation/2013/02/13/online-dating-mobile-apps/1902011/. The mobile dating market grew to almost $213 million in 2012, and analysts expect the mobile dating market to nearly double within five years. *Id*. Currently, popular dating websites provide the app for free but require users to pay subscription fees to access their online profile information via the mobile app. *Id*.

21 Quentin Fottrell, *10 Things Dating Sites Won't Tell You: The Risks and Rewards of Looking for Love Online*, MARKET WATCH (Feb. 11, 2013, 10:24 AM), http://articles.marketwatch.com/2013-02-11/finance/36988343_1_match-com-okcupid-online-personals-watch. However, both Match.com and eHarmony offer discounted rates for a six-month bundle. *Id*.

22 *See Here's How Chemistry Works for You*, CHEMISTRY.COM, http://www.chemistry.com/tour (last visited June 9, 2013) (requiring users to take a personality test and to receive personalized matches based on the test); PLENTYOFFISH, http://www.pof.com (last visited June 9, 2013) (matching users based on a "Chemistry Test"); *Scientific Match Making*, EHARMONY, http://www.eharmony.com/why/science-of-compatibility/ (last visited June 9, 2013) (recognizing that the compatibility matching system takes into account twenty-nine compatibility dimensions to predict a user's possible relationship success).

23 *The Perils and Pitfalls of Online Dating: How to Protect Yourself*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/fs/fs37-online-dating.htm (last updated May 2013). Additionally, dating websites may retain the information after an individual deletes his or her account. *See* Robert L. Mitchell, *Online Dating: Your Profile's Long, Scary Shelf Life*, COMPUTERWORLD (Feb. 13, 2009, 12:00 PM), https://www.computerworld.com/s/article/9127799/Online_dating_Your_profile_s_long_scary_shelf_life (explaining the length of time that dating websites retain user information after the user deletes the profile). True.com retains user information indefinitely, and eHarmony archives user information but does not delete a user from the database. *Id*. Alternatively, PlentyOfFish deletes "records after six months to a year of inactivity." *Id*. Dating website eHarmony retains user information because many users return to the service after inactivity and retaining the information prevents users from filling out the several hundred profile questions again. *Id.* However, dating websites also retain the information because companies find it valuable for marketing purposes. *Id*.

behavior; (3) sexual preferences; and (4) income.[24] Although websites use this information to recommend specific users as potential dates, most websites fail to perform criminal background checks to screen for users with past sexual assault or violent crime convictions.[25]

Additionally, online dating websites' terms of use waive the website's liability for any damages arising from the conduct of the user or anyone else in connection with using the service.[26] To help users avoid dangerous situations arising from online dating, websites provide safety tips as guidelines for a safe and successful experience.[27] However,

---

[24] *The Perils and Pitfalls of Online Dating: How to Protect Yourself*, *supra* note 23. Although users expect their online contacts to view their information, third parties may access the information as well. *See Social Networking Privacy: How to be Safe, Secure and Social*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/social-networking-privacy#access (last updated May 2013) (explaining who may access user profile information posted on social networking sites). Users expect their contacts on social networking sites to access their information; however, additional parties including (1) advertisers, (2) software developers, (3) identity thieves, and (4) other online criminals, may access information with legal or illegal motives. *Id.* Furthermore, users should provide accurate information because litigation increasingly involves the use of dating website profile information. *Dating Website Info Being Used in Divorces*, UPI.COM (Feb. 17, 2013, 11:02 PM), http://www.upi.com/Top_News/US/2013/02/17/Dating-website-info-being-used-in-divorces/UPI-73261361160121/?spt=hs&or=tn. A survey polling top divorce attorneys discovered 59% of the attorneys noticed an increase in the use of dating website information during divorce proceedings. *Id.* Most commonly parties use information relating to an individual's relationship status. *Id.* In addition, attorneys use information about a party's salary, occupation, and parental status to show deceit or lack of honesty. *Id.*

[25] *See Match.com Terms of Use Agreement*, MATCH.COM, http://www.match.com/registration/membagr.aspx?lid=4 (last revised May 16, 2013) (warning users that Match.com does not perform criminal background checks); *PlentyOfFish Terms of Use Agreement*, PLENTYOFFISH, http://www.pof.com/terms.aspx (last updated May 31, 2013) (stating that PlentyOfFish does not perform criminal background checks); *Terms of Service*, EHARMONY, http://www.eharmony.com/about/terms/ (last visited June 9, 2013) (explaining that eHarmony does not perform criminal background checks on users). *But see About True*, TRUE, http://www.true.com/about.htm?svw=homepage (last visited June 9, 2013) (screening all communicating members through the largest criminal records databases online).

[26] *See, e.g.*, *Match.com Terms of Use Agreement*, *supra* note 25; *PlentyOfFish Terms of Use Agreement*, *supra* note 25; *Terms of Service*, *supra* note 25.

[27] *See, e.g.*, *Good Advice–Safety Tips to Follow*, MATCH.COM, http://www.match.com/help/safetytips.aspx?lid=4 (last visited June 9, 2013) (warning users to protect their finances and online information, to get to know someone before meeting in person, and to provide their own transportation to and from the date); *Safety Tips*, EHARMONY, http://www.eharmony.com/safe-online-dating/ (last visited June 9, 2013) (warning users to research and screen their dates, to choose a public place for initial dates, and to tell family or friends about their plans). Reports suggest 62% of dating website users research their dates before meeting in person, and among 18- to 24-year-olds the percentage increases to 71%. *Match-Making Sites Making Blind Dating a 'History'*, TIMES OF INDIA (Oct. 24, 2012, 1:02 PM), http://articles.timesofindia.indiatimes.com/2012-10-24/computing/34707223_1_blind-date-first-date-match-com.

providing users with online and offline dating safety tips has failed to prevent criminal attacks.[28] In 2011, a California woman alleged her date, whom she met on Match.com, sexually assaulted her after a second date, and the woman's attorney stated that the man had six prior convictions for sexual battery.[29] Although online dating creates an environment for

---

[28] *See, e.g.*, KC Kelly, *Wade Ridley Assaults Match.com Date, Mary Kay Beckman: Online Dating Safety Tips*, EXAMINER.COM (Feb. 16, 2011), http://www.examiner.com/article/wade-ridley-assaults-match-com-date-mary-kay-beckman-online-dating-safety-tips (explaining how Wade Ridley stabbed and beat his online date after she ended their relationship); Ryan Raiche, *Experts: Emotions and Feelings Can Lead to Poor Decisions When Involved in an Online Romance*, ABC ACTION NEWS (Sept. 18, 2012), http://www.abcactionnews.com/dpp/news/local_news/experts-emotions-and-feelings-can-lead-to-poor-decisions-when-involved-in-an-online-romance (discussing the attack and robbery of Joseph Bruno by his online date Bobbie Jo Curtis and her son and friend); *see also* Jessica S. Groppe, Comment, *A Child's Playground or a Predator's Hunting Ground? – How to Protect Children on Internet Social Networking Sites*, 16 COMMLAW CONSPECTUS 215, 227–28 (2007) (highlighting the risks involved with children using social networks and discussing how predators may take advantage of children online). *But see* Lawrence G. Walters, *Shooting the Messenger: An Analysis of Theories of Criminal Liability Used Against Adult-Themed Online Service Providers*, 23 STAN. L. & POL'Y REV. 171, 211–12 (2012) (arguing that websites should be granted immunity from the actions of criminals using websites to further criminal activity). However, beyond criminal attacks, dating website users also succumb to financial scams. *See* Fottrell, *supra* note 21 (noting that dating website users suffered large financial losses by online scams). Reports state users lost $50 million in 2011 from romance scams with the average victim losing nearly $9000. *Id*.

[29] Chris Sedens, *Woman Sues Match.com After Alleged Sex Assault by Man She Met Online*, CBS L.A. (Apr. 14, 2011, 7:37 AM), http://losangeles.cbslocal.com/2011/04/14/woman-sues-match-com-after-sex-assault-by-man-she-met-online/. The woman sued Match.com and requested the site implement a sexual predator screening process. *Id*. For additional instances of women being sexually assaulted by their online dates, see Richard Alleyne, *Personal Trainer Raped, Beat and Robbed Secretary He Met on Dating Website*, TELEGRAPH (May 25, 2012), http://www.telegraph.co.uk/news/uknews/crime/9290437/Personal-trainer-raped-beat-and-robbed-secretary-he-met-on-dating-website.html, reporting the rape and assualt of a woman by an online date from PlentyOfFish.com, and Jason Meisner, *Online Dates Led to Rape, Police Say PR Executive Charged with Assaulting Women He Met Through Dating Website*, CHI. TRIB., Sept. 10, 2011, http://www.articles.chicagotribune.com/2011-09-10/news/ct-met-online-assault-west-suburban-woman-website, discussing how Ignacio Carrillo sexually assaulted two women he met through an online dating website. Violence against women predominately occurs from the actions of an intimate partner. Wendy Pollack, *Teen Dating Violence and the Subtle (and Not So Subtle) Blaming of Victims*, SHRIVER BRIEF (Feb. 25, 2013, 10:08 AM), http://www.theshriverbrief.org/2013/02/articles/womens-law-and-policy/teen-dating-violence-and-the-subtle-and-not-so-subtle-blaming-of-victims/ (indicating that the biggest threat of sexual violence to women may result from their romantic partner). In 2009, 79% of reported rapes and sexual assaults against women were committed by a person the victim knew, and 41% of the attacks were committed by a current or former partner. *Id.* Estimates indicate that over 50 million people each year suffer some form of sexual or intimate partner violence. Wendy Pollack, *Increasing Sexual Violence Is a Serious Public Health Issue*, SHRIVER BRIEF (Feb. 6, 2012, 1:45 PM), http://www.theshriverbrief.org/2012/02/articles/womens-law-and-policy/increasing-sexual-violence-is-a-serious-public-health-issue/. Additionally, it is estimated 53.2 million women are raped in their lifetime. *Id*.

dangerous criminal attacks to occur, most states only regulate how dating websites contract with users, rather than enacting statutes to reduce the probability of criminal attacks stemming from online dating.[30]

B. State Statutes Affecting Online Dating Websites

With the increase in dating website use and the potential dangers associated with online dating, states enacted statutes to protect users from harmful business practices and to warn users of potential dangers.[31] Part II.B.1 provides an overview of state statutes designed to protect users when contracting with dating websites.[32] Part II.B.2 discusses state statutes enacted to improve user safety while utilizing dating websites.[33]

1. Statutes Regulating Dating Website Contracts

The majority of state statutes involving dating websites impose requirements on the websites when contracting with users.[34] For example, states require dating websites to provide users with a copy of the contract and allow users three business days to rescind the contract.[35]

---

30 *See infra* Part II.B (examining the state statutes that govern dating websites).

31 *See infra* Parts II.B.1–2 (listing state statutes that protect users from deceptive or poor business practices of dating websites and explaining state statutes that require websites to warn users about criminal background check usage).

32 *See infra* Part II.B.1 (discussing state statutes that affect user contracts and billing practices with dating websites).

33 *See infra* Part II.B.2 (providing an in-depth look into state statutes that require dating websites to notify users about whether the website performs criminal background checks and about the risks and dangers of criminal background checks).

34 *See* Phyllis Coleman, *Online Dating: When "Mr. (Or Ms.) Right" Turns Out All Wrong, Sue the Service!*, 36 OKLA. CITY U. L. REV. 139, 144–57 (2011) (examining state statutes regulating dating websites); *see also, e.g.*, ARIZ. REV. STAT. ANN. §§ 44-7152 to -7154 (West, WestlawNext through legislation effective June 20, 2013 of the 1st Reg. Sess. of the 51st Leg.) (requiring websites to allow rescission within three business days, outlining the requirements for a contract, and recognizing prohibited contract provisions); CAL. CIV. CODE §§ 1694.1–.4 (West, WestlawNext current with urgency legislation through ch. 70 of 2013 Reg. Sess.) (stating contracts are void if entered into based on fraudulent or misleading information and outlining other contractual provisions relating to cancellation, refunds, death, and relocation); CONN. GEN. STAT. ANN. § 42-321 (West, WestlawNext current with Public Acts enrolled and approved by the Governor on or before June 1, 2013 and effective on or before July 1, 2013) (requiring the website to provide a copy of the contract to the user).

35 ARIZ. REV. STAT. ANN. §§ 44-7152 to -7153 (mandating that dating websites provide customers with a copy of their contract and allow users three business days to rescind the contract); CAL. CIV. CODE § 1694.2 (requiring that dating websites provide customers with a copy of their contract, include specific language regarding the cancellation policy in the contract, and provide customers a rescission period of three business days); CONN. GEN. STAT. ANN. § 42-321 (stating clients must receive a copy of their contract, the website must allow a rescission period of three business days, and the website must return client money

Additionally, some states protect users from fraudulent contracts or deceitful business practices by declaring those contracts void and unenforceable.[36] Furthermore, some states limit the length of dating website contracts and the fees that a dating website may charge users.[37] Although these statutes protect users from fraudulent business practices, other statutes provide protection from criminal attacks.[38]

---

within ten business days of a cancelled agreement); 815 ILL. COMP. STAT. ANN. 615/20 (West, WestlawNext through P.A. 98-21 of the 2013 Reg. Sess.) (providing users with a rescission period of three business days); IOWA CODE ANN. §§ 555A.2–A.3 (West, WestlawNext current with immediately effective legislation signed as of May 21, 2013 from the 2013 Reg. Sess.) (requiring dating websites to provide a copy of the contract and granting three business days for cancellations); N.Y. GEN. BUS. LAW § 394-c (McKinney, WestlawNext through L.2013, ch. 1 to 57 and 60 to 110) (mandating that referral services provide customers with a copy of the agreement, notify customers about a three business day cancellation policy, and limit contracts to two-year terms); N.C. GEN. STAT. ANN. § 66-119 (West, WestlawNext through S.L. 2013-70 of the 2013 Reg. Sess. of the Gen. Assemb.) (allowing customers three business days to cancel their contract and requiring companies to provide customers with a copy of the agreement); OHIO REV. CODE ANN. §§ 1345.42–.43 (West, WestlawNext through 2013 File 17 of the 130th GA (2013-2014)) (requiring that businesses provide customers with a copy of the contract and allow a rescission period of three business days); R.I. GEN. LAWS ANN. § 5-78-2(a) to (b)(1) (West, WestlawNext through chapter 491 of the Jan. 2012 session) (stating that customers must receive a copy of the contract and granting customers a cancellation period of three business days); WIS. STAT. ANN. § 100.175 (West, WestlawNext through 2013 Wisconsin Act 19, published May 18, 2013) (mandating that dating services provide contracts to customers, allow customers three business days to rescind, and return refunds within twenty-one days of cancellation).

[36] *See* CAL. CIV. CODE § 1694.4(a)–(b), (e) (declaring contracts entered into on fraudulent or deceitful information void and also declaring a contract void if the buyer waives benefits imposed by the statute); 815 ILL. COMP. STAT. ANN. 615/40 (prohibiting contracts based on unfair practices and declaring those contracts "void and unenforceable").

[37] *See* ARIZ. REV. STAT. ANN. § 44-7154 (restricting a dating service's contract to one year but allowing the service to provide customers with an option to renew for one year thereafter); CAL. CIV. CODE § 1694.2(d) (prohibiting contracts requiring customers to pay beyond two years from the date of the contract but allowing the contract to provide services extending up to three years from the date of the contract); 815 ILL. COMP. STAT. ANN. 615/30(a) (limiting contracts to two years with an option to renew for a period not to exceed one year); N.Y. GEN. BUS. LAW § 394-c (limiting the contract to two years, limiting fees to $1000, requiring sellers who charge more than $25 to provide a specific number of monthly referrals, and allowing buyers to cancel the contract and receive a refund if the service fails to meet the required number of referrals for two consecutive months); N.C. GEN. STAT. ANN. § 66-123(a) (limiting contract duration to three years); WIS. STAT. ANN. § 100.175(5)(a) (prohibiting contracts from requiring a buyer to pay more than $100 for dating services before the buyer receives the services, unless the seller establishes proof of financial responsibility).

[38] *See infra* Part II.B.2 (demonstrating how a few state statutes focus on protecting users from harmful or criminal users online).

2. Statutes Designed to Increase Online Dating Safety

Rather than focusing on contracts or business practices, a few states enacted statutes specifically designed to provide awareness to users about the dangers of online dating.[39] The statutes require a website to state whether it performs criminal background checks, identify whether it allows users with criminal backgrounds to use the site, and also mandates that websites warn users that criminal background checks fail to flag all dangerous individuals.[40] Additionally, the statutes require dating sites to list and describe safety measures used to develop safer dating practices.[41] The statutes address the effectiveness of criminal background checks, by warning users of the inadequacies of background checks, so users remain cautious when using a dating website.[42]

---

[39] *See* Coleman, *supra* note 34, at 149 (recognizing the distinctions between New Jersey's statute from other statutes regulating dating websites); *see also, e.g.*, 815 ILL. COMP. STAT. ANN. 518/10 (requiring online dating services to notify users about safety awareness and criminal background checks); N.Y. GEN. BUS. LAW § 394-cc(2) (requiring dating websites to notify users about safety measures); TEX. BUS. & COM. CODE ANN. § 106.006 (West, WestlawNext through Chapters effective immediately through Chapter 36 of the 2013 Reg. Sess. of the 83rd Leg.) (requiring dating websites to notify users about safety measures). New Jersey created a unique statute requiring dating websites to notify users about whether the site conducts criminal background checks. Coleman, *supra* note 34, at 149. Kevin Ambler attempted to sponsor a similar statute in Florida, but failed four times. Diane C. Lade, *The Sweetheart Swindle*, S. FLA. SUN-SENTINEL, Mar. 31, 2008, at 1D, *available at* 2008 WLNR 6061176; *see supra* note 25 and accompanying text (providing examples of popular dating websites that adopted policies similar to New Jersey's statute and now notify users whether the site conducts criminal background checks).

[40] *See, e.g.*, 815 ILL. COMP. STAT. ANN. 518/10(b)–(d); N.J. STAT. ANN. § 56:8-171 (West, WestlawNext through L.2013, c. 84 and J.R. No. 9); TEX. BUS. & COM. CODE ANN. §§ 106.004(a)–.005(b). The statutes work in tandem with current safety procedures used by dating websites to create awareness about the dangers of online dating. *See supra* note 27 (explaining how dating websites provide safety tips for successful online dating and recommend that all users proceed with caution). However, opponents of New Jersey's statute, including the Internet Alliance, believe the statute may increase the problem by creating "a false sense of security." *See* Lade, *supra* note 39 (discussing the Internet Alliance's executive director's concerns regarding the New Jersey statute and how it may affect user safety).

[41] *See, e.g.*, 815 ILL. COMP. STAT. ANN. 518/10(a); N.J. STAT. ANN. § 56:8-171a; N.Y. GEN. BUS. LAW § 394-cc2; TEX. BUS. & COM. CODE ANN. § 106.006. Additionally, the New Jersey statute provides examples of proper safety notifications including: (1) recognizing that identity thieves may create false profiles; (2) using caution when communicating with and meeting a stranger; (3) refusing to provide other users with personal contact information beyond the scope of the site; and (4) notifying a third party when meeting with strangers, utilizing separate transportation, and meeting in a public place. N.J. STAT. ANN. § 56:8-171a.

[42] *See, e.g.*, N.J. STAT. ANN. §§ 56:8-169 to -173 (requiring dating websites to notify users whether the website performs criminal background checks); *see also* Coleman, *supra* note 34, at 150 (explaining how the New Jersey statute responds to critics, who argue the notification will create a false sense of security). Specifically, the New Jersey statute

Although states enacted statutes imposing duties on dating websites, courts interpreted the CDA as granting immunity to websites, including dating services, from tort and negligence actions.[43]

C. The CDA and the Internet Evolution

In 1996, Congress enacted the CDA to promote the development and preserve the free market of the Internet.[44] Since the CDA's enactment, the Internet evolved and now individuals utilize it for many daily tasks.[45] Part II.C.1 explains the purpose of the CDA and provides a brief history of early CDA interpretations.[46] Part II.C.2 notes the changes in the Internet since the CDA's enactment and discusses how the Internet encompasses a large portion of society's daily lives.[47]

1. CDA History and Its Initial Application

Congress designed section 230 of the CDA to allow websites to block and filter third-party content without incurring liability.[48] To accomplish that goal, the CDA prevents courts from treating a provider or user of an Interactive Computer Service ("ICS") as the publisher or speaker of

---

requires dating websites that conduct criminal background checks to state: (1) criminal background checks fail to flag all dangerous individuals; (2) users may rely too much on the belief that checks catch all dangerous individuals; (3) criminals may develop methods of circumventing the checks; (4) not all states make criminal records public; (5) states may update criminal records databases infrequently; (6) the checks only include publicly available convictions; and (7) domestic databases do not check foreign arrests and convictions. N.J. STAT. ANN. § 56:8-171d.

43 *See infra* Part II.C.1 (discussing the CDA and how courts use the CDA to dismiss tort actions against websites).

44 47 U.S.C. § 230(b)(1)–(2) (2006); *see* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 57–58 (1996) (providing an overview of the CDA and its legislative history).

45 *See infra* Part II.C.2 (examining the Internet evolution and how society substantially increased its Internet usage since the CDA's enactment).

46 *See infra* Part II.C.1 (highlighting the CDA's enactment and its initial application).

47 *See infra* Part II.C.2 (discussing the evolution of the Internet and how it shapes much of our daily lives).

48 *See* Cannon, *supra* note 44, at 53 (discussing Senator Exon's motivation for sponsoring the CDA); Cara J. Ottenweller, Note, *Cyberbullying: The Interactive Playground Cries for a Clarification of the Communications Decency Act*, 41 VAL. U. L. REV. 1285, 1303 (2007) (identifying that section 230(c)(3) grants certain eligible parties "immunity from civil liability for attempting to restrict objectionable material posted by third parties."). Senator Exon proclaimed the Internet grants children access to pornography; therefore, he proposed the CDA to regulate speech on the Internet. Cannon, *supra* note 44, at 53.

information provided by another content provider.[49] To do this, the CDA distinguishes between an ICS and an Information Content Provider ("ICP") when granting immunity.[50] Courts developed a three-prong test to determine whether a website deserves immunity under the CDA: (1) whether the website qualifies as an ICS; (2) whether the action treats the defendant as the publisher or speaker of information for liability purposes; and (3) whether a third party provided the information.[51] In 1997, the Fourth Circuit decided the first case interpreting section 230 of the CDA.[52]

In *Zeran v. America Online, Inc.* ("AOL"), someone anonymously posted on an AOL message board an advertisement to purchase "Naughty Oklahoma T-Shirts" after the Oklahoma City bombing and instructed purchasers to call Ken Zeran at his home phone number.[53] Zeran sued AOL and claimed a duty existed to remove the posting, notify users the messages were false, and screen more effectively for

---

[49] 47 U.S.C. § 230(c)(1); *see* Trenton E. Gray, Comment, *Internet Dating Websites: A Refuge for Internet Fraud*, 12 FLA. COASTAL L. REV. 389, 397 (2011) (distinguishing between an ICS and an ICP under the CDA); KrisAnn Norby-Jahner, Comment, "*Minor*" *Online Sexual Harassment and the CDA § 230 Defense: New Directions for Internet Service Provider Liability*, 32 HAMLINE L. REV. 207, 232–34 (2009) (explaining the intent behind the CDA and how the CDA allows ICS's to filter third-party content without incurring liability for the content).

[50] 47 U.S.C. § 230(f)(2)–(3) (defining an ICS as a service or system that allows multiple users to access the Internet and defining an ICP as a person or entity responsible for creating or developing information provided through the Internet or other ICS). An ICS is granted immunity under the CDA while an ICP is not granted immunity. *Id.* § 230(c)(2); *see* Gray, *supra* note 49, at 397 (explaining the distinction between an ICS and ICP by demonstrating that the CDA grants immunity to an ICS for third-party actions but does not similarly grant immunity to an ICP). *See generally* Jay M. Zitter, Annotation, *Civil Liability of Internet Dating Services*, 48 A.L.R.6th 351 (2009) (overviewing the different possible causes of action users may bring against internet dating websites).

[51] *See* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 412 (2010) (providing the elements used by courts to determine immunity under the CDA). However, the Ninth Circuit may have created an additional fourth prong based on whether the defendant promised to remove content yet failed to do so. *Id.*; *see* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1107–09 (9th Cir. 2009) (adding a possible fourth prong based on the website's promise, but failure, to remove posted content).

[52] Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997); *see* Bradford J. Sayler, Comment, *Amplifying Illegality: Using the Exception to CDA Immunity Carved Out by* Fair Housing Council of San Fernando Valley v. Roommates.com *to Combat Abusive Editing Tactics*, 16 GEO. MASON L. REV. 203, 210–12 (2008) (discussing *Zeran v. AOL* and its broad grant of immunity).

[53] 129 F.3d at 329. *See generally* Patricia Spiccia, Note, *The Best Things in Life are Not Free: Why Immunity Under Section 230 of the Communications Decent Act Should Be Earned and Not Freely Given*, 48 VAL. U. L. REV. 369 (2013) (discussing the decision in *Zeran*). Zeran received many calls where individuals left angry messages including death threats. *Zeran*, 129 F.3d at 329. Zeran called AOL requesting that AOL remove the posts, however AOL refused to issue a retraction declaring the posting a hoax. *Id.*

defamatory material.[54] In response, AOL raised section 230 of the CDA as an affirmative defense.[55] The court granted AOL immunity under the CDA because AOL qualified as an ICS and Zeran attempted to hold AOL liable as a publisher of information from a third party.[56] Following *Zeran*, courts relied on the Fourth Circuit's reasoning to grant immunity to websites in a broad range of cases.[57] Although many courts continue to rely on *Zeran* when determining CDA immunity, the Internet has evolved dramatically since the *Zeran* decision.[58]

---

54 *Zeran*, 129 F.3d at 329–30.

55 *Id*. at 330; *see* Cecilia Ziniti, Note, *The Optimal Liability System for Online Service Providers: How* Zeran v. America Online *Got it Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583, 585–87, 594 (2008) (explaining the *Zeran* opinion, discussing how *Zeran* created a three-part test for section 230 immunity, and arguing that the *Zeran* approach best serves web 2.0 by granting broad immunity).

56 *Zeran*, 129 F.3d at 332–33. Zeran argued AOL was liable as a distributor because AOL knew of the defamatory postings; but, the court failed to find a distinction between publishers and distributors of information. *Id*. at 331–32. Many courts rely on the *Zeran* Court's reasoning and ultimately grant broad immunity under the CDA. *See, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008) (granting immunity to social networking website MySpace); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1125 (9th Cir. 2003) (expanding the CDA by granting immunity to a dating website). *See generally* Ziniti, *supra* note 55 (arguing that *Zeran*'s broad grant of immunity best serves the current state of the Internet).

57 *See, e.g.*, Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 418–19 (1st Cir. 2007) (finding Lycos, Inc. immune under the CDA in an action involving defamatory postings by third parties on a Lycos, Inc. message board); Doe v. GTE Corp., 347 F.3d 655, 656, 659 (7th Cir. 2003) (holding GTE immune, as an ISP, when it displayed images of athletes while in the locker room setting, without the athletes knowing of the recording); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 716 (Ct. App. 2002) (barring a negligence action against eBay because the content provided was created by third parties). However, some courts decided not to grant immunity, thus creating exceptions to the *Zeran* reasoning. *See, e.g.*, FTC v. Accusearch Inc., 570 F.3d 1187, 1201 (10th Cir. 2009) (deciding not to grant immunity to Accusearch Inc. under the CDA from a suit for selling personal data that included telephone records); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008) (choosing not to grant immunity to Roommates.com, after holding Roommates.com was an ICP because the site's activity involved asking potentially unlawful questions). In *Roommates.com*, the website enabled users to search for roommates based on specific qualifications; however, the questionnaire provided by the website included questions about race, thus making the questionnaire potentially illegal under the Fair Housing Act. *Id.* at 1164; *see* Jeffrey R. Doty, Comment, *Inducement or Solicitation? Competing Interpretations of the "Underlying Illegality" Test in the Wake of* Roommates.com, 6 WASH. J.L. TECH. & ARTS 125, 130–31 (2010) (providing an overview of the underlying illegality approach to determine whether a website may be immune under the CDA when the website contributes to or solicits illegal activity); Sayler, *supra* note 52, at 214 (proposing that courts apply *Roommates.com*'s reasoning to defamatory editing tactics); Rachel Seaton, Comment, *All Claims Are Not Created Equal: Challenging the Breadth of Immunity Granted by the Communications Decency Act*, 6 SETON HALL CIR. REV. 355, 369–75 (2010) (discussing *Roommates.com* and its effect on CDA analysis).

58 *See infra* Part II.C.2 (explaining how the Internet has changed since the CDA's enactment).

2. The Internet Evolution

When Congress enacted the CDA, it chose to protect the Internet more than the individuals using the Internet.[59] However, Congress did not likely foresee the Internet boom and the infiltration of the Internet into much of our daily lives.[60] In 1995, a year before the CDA's enactment, the Internet user base consisted of less than 40 million people and less than 23,500 websites; however, in 2011, nearly 2 billion people accessed the Internet, which then consisted of nearly 300 million websites.[61] Due to greater accessibility, people now use the Internet for information, shopping, education, communication, entertainment, and banking, among other uses.[62] In addition to the Internet's increased capabilities, smart phones allow people to access the Internet

---

59 Gray, *supra* note 49, at 398.

60 *See* Lumturije Akiti, Note, *Facebook Off Limits? Protecting Teachers' Private Speech on Social Networking Sites*, 47 VAL. U. L. REV. 119, 122–23 (2012) (noting that Facebook reached 750 million active users worldwide and 157 million users in the United States in July 2011); Suzanne Choney, *25 Percent Use Smartphones, Not Computers, for Majority of Web Surfing*, NBC NEWS (July 11, 2011), http://www.nbcnews.com/technology/technolog/25-percent-use-smartphones-not-computers-majority-web-surfing-122259 (discussing that more people access the Internet on the go, rather than using a computer); Megan Gannon, *Why Some Facebook Users Constantly Update Status*, LIVESCIENCE (Jan. 3, 2013, 5:13 PM), http://www.livescience.com/25972-facebook-status-updates-loneliness.html (explaining how many people use Facebook constantly throughout the day); Donald Melanson, *Amazon Announces Q4 2011 Results: Sales Jump to $17.43 Billion, but Profits Drop 58 Percent*, ENGADGET (Jan. 31, 2012, 4:26 PM), http://www.engadget.com/2012/01/31/amazon-announces-q4-2011-results-sales-jump-to-17-43-billion/ (overviewing the amount of online sales on Amazon.com). CDA litigation primarily revolves around ISPs that simply provide a message board for users to post comments. *See, e.g.*, *Zeran*, 129 F.3d at 329 (deciding CDA immunity for an ISP that provided message boards for users to interact with each other); Doe v. Am. Online Inc., 783 So. 2d 1010, 1011–12 (Fla. 2001) (hearing a case regarding "chat rooms" and the application of the CDA).

61 *The Rather Petite Internet of 1995*, PINGDOM (Mar. 31, 2011), http://royal.pingdom.com/2011/03/31/internet-1995/. In 2011, the Internet user base was 50 times larger than in 1995, and the number of Facebook users was "15 times larger than the entire Internet was in 1995." *Id.*; *see* Shelbie J. Byers, Note, *Untangling the World Wide Weblog: A Proposal for Blogging, Employment-At-Will, and Lifestyle Discrimination Statutes*, 42 VAL. U. L. REV. 245, 250–51 (2007) (highlighting the increase in popularity of blogs by noting that web users create thousands of blogs daily and maintain millions of other blogs as well).

62 *See* Hemangi Harankhedkar, *Internet and Its Uses in Our Daily Life*, BUZZLE (Aug. 17, 2011), http://www.buzzle.com/articles/internet-and-its-uses-in-our-daily-life.html (listing how society uses the Internet for daily tasks); *see also* Gannon, *supra* note 60 (explaining that college students rely on Facebook for communication purposes); Melanson, *supra* note 60 (discussing the growth in online shopping via Amazon). Although the Internet provides many benefits, including the ability to connect across the globe with social networking, the increasing use of social networking sites poses new problems for the legal community. *See generally* Emily M. Janoski-Haehlen, *The Courts Are All a 'Twitter': The Implications of Social Media Use in the Courts*, 46 VAL. U. L. REV. 43 (2011) (identifying problems raised by social networking sites for courts, judges, and attorneys).

anywhere.[63] Furthermore, the Internet led to the creation of new industries supporting companies with large revenues and profits.[64] However, courts rely on reasoning from the 1990s when deciding and interpreting the CDA.[65] Throughout the Internet evolution plaintiffs used tort actions in an attempt to hold dating websites accountable for their injuries.[66]

D. Tort Actions Against Dating Websites

Individuals attempting to sue an online dating or social networking website generally use one of three causes of action: (1) negligence; (2) fraud; or (3) negligent misrepresentation.[67] Most cases brought under these theories result in the court granting the website immunity under the CDA.[68] Part II.D.1 reviews the necessary elements for negligence,

---

[63] *See* Choney, *supra* note 60 (explaining the increase in people that use a smartphone to access the Internet rather than a computer); *see also* Brian Honigman, *100 Fascinating Social Media Statistics and Figures from 2012*, HUFFINGTON POST (Nov. 29, 2012, 7:32 PM), http://www.huffingtonpost.com/brian-honigman/100-fascinating-social-me_b_2185281.html (providing statistics that illustrate the increase in mobile access to social networking sites). Nearly 500 million users regularly access Facebook via their smartphone and 50% of Twitter users access Twitter via its mobile site. *Id*.

[64] *See* Michael Berkens, *IAC Reports Earnings: Match.com Up 22%: IAC Renews Search Deal with Google & Has $1.6 Billion in Cash*, DOMAINS (Apr. 26, 2011), http://www.thedomains.com/2011/04/26/iac-reports-earnings-match-com-up-22-iac-renews-search-deal-with-google-has-1-6-billion-in-cash/ (overviewing Match.com's increasing revenue and profits); Claire Cain Miller, *Google Still in a Struggle with Mobile*, N.Y. TIMES (Jan. 22, 2013), http://www.nytimes.com/2013/01/23/technology/google-profit-exceeds-expectations.html?_r=0 (noting Google's billions in profit even though the company struggles with the emerging mobile market); *see also supra* note 20 and accompanying text (discussing the growth and profitability of online dating).

[65] *See, e.g.*, Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 252, 254, 260 (4th Cir. 2009) (relying on *Zeran* to grant immunity to a website allowing buyers to comment on goods they purchased); Doe v. MySpace, Inc., 528 F.3d 413, 419–20 (5th Cir. 2008) (using the *Zeran* court's reasoning to grant MySpace immunity under the CDA); Doe II v. MySpace, Inc., 96 Cal. Rptr. 3d 148, 153–54, 159 (Ct. App. 2009) (granting immunity to MySpace based on the *Zeran* approach).

[66] *See infra* Part II.D (explaining the necessary elements of common law tort actions filed against dating websites and discussing negligence actions involving dating websites).

[67] *See, e.g.*, *Doe*, 528 F.3d at 417 (identifying that plaintiffs filed a negligence claim and a gross negligence claim against MySpace); Doe v. SexSearch.com, 502 F. Supp. 2d 719, 729 (N.D. Ohio 2007) (discussing plaintiff's fraud claim against a website), *aff'd*, 551 F.3d 412 (6th Cir. 2008); Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257, 1262 (N.D. Cal. 2006) (reviewing plaintiff's fraud and negligent misrepresentation claims against Yahoo!), *aff'd*, 376 F. App'x. 775 (9th Cir. 2010).

[68] *See, e.g.*, *Doe*, 528 F.3d at 421 (barring all of plaintiff's claims under the CDA); *SexSearch.com*, 502 F. Supp. 2d at 728 (granting SexSearch.com immunity under the CDA). *But see Anthony*, 421 F. Supp. 2d at 1262–63 (finding that the CDA did not bar the fraud and negligent misrepresentation claims).

fraud, and negligent misrepresentation.[69] Part II.D.2 discusses cases that involve interactive websites and the CDA.[70]

1. Types of Tort Actions

Negligence covers unreasonably risky behavior that causes harm.[71] To prove a claim of negligence, a plaintiff must establish five elements: (1) a duty of care owed by the defendant to the plaintiff; (2) the defendant's breach of the duty of care owed to the plaintiff; (3) an injury or loss sustained by the plaintiff; (4) causation in fact; and (5) proximate cause.[72] A duty of care may exist under a reasonable care standard or through a statute designed to protect against a specific type of conduct.[73]

---

69 *See infra* Part II.D.1 (discussing the required elements for negligence, fraud, and negligent misrepresentation).

70 *See infra* Part II.D.2 (explaining court decisions interpreting CDA immunity for interactive websites).

71 DAN B. DOBBS, PAUL T. HAYDEN & ELLEN M. BUBLICK, THE LAW OF TORTS § 2 (2d ed. 2011) (defining the tort of negligence).

72 *See* Hale v. Ostrow, 166 S.W.3d 713, 716 (Tenn. 2005) (listing the required elements for a negligence action); *see also* Gipson v. Kasey, 150 P.3d 228, 230 (Ariz. 2007) (listing four elements a plaintiff must prove for a negligence cause of action); RESTATEMENT (SECOND) OF TORTS § 284 (1965) (defining negligent conduct as either "an act which the actor as a reasonable man should recognize as involving an unreasonable risk of causing an invasion of an interest of another, or . . . a failure to do an act which is necessary for the protection or assistance of another and which the actor is under a duty to do").

73 RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM §§ 7, 14 (2010) (recognizing that a person ordinarily maintains a duty to exercise reasonable care and that a person is negligent *per se* if they violate a statute created to protect against the particular accident caused by the actor's conduct and if the statute protects a class of persons that includes the victim); *see* O'Guin v. Bingham Cnty., 122 P.3d 308, 311 (Idaho 2005) (defining the necessary elements of negligence *per se*); Chaffin v. Brame, 64 S.E.2d 276, 279 (N.C. 1951) (expressing the reasonable care standard as "[w]hat would a reasonably prudent person have done under the circumstances as they presented themselves"); RESTATEMENT (SECOND) OF TORTS § 283 (1965) (explaining the reasonable care standard). However, in some situations a duty of care may involve protecting people from the criminal acts of third parties. Boren v. Worthen Nat'l Bank of Ark., 921 S.W.2d 934, 939–40 (Ark. 1996). Courts apply three tests to determine whether a duty exists to protect another from the criminal acts of third parties: (1) the Specific Harm Test; (2) the Prior Similar Incidents Test; or (3) the Totality of the Circumstances Test. *Id.* at 940–41. The Specific Harm Test imposes a duty when the business owner knows or has reason to know of acts occurring or about to occur that pose an imminent probability of harm. *Id.* at 940; *see, e.g.*, Fuga v. Comerica Bank-Detroit, 509 N.W.2d 778, 779 (Mich. Ct. App. 1993) (applying the Specific Harm Test to an action brought by a plaintiff who was injured by a third party while using the defendant's ATM); Cornpropst v. Sloan, 528 S.W.2d 188, 198 (Tenn. 1975) (applying the Specific Harm Test in a negligence case that involved a female shopper who was assaulted in a parking lot). The Prior Similar Incidents Test imposes a duty when a particular crime becomes foreseeable based on the similarity, frequency, location, and proximity of prior criminal acts. *Boren*, 921 S.W.2d at 940–41; *see* Williams v. First Ala. Bank, 545 So. 2d 26, 27 (Ala. 1989) (finding two prior robberies insufficient to impose a duty and holding that a

An actor breaches a legal duty by accepting an unreasonable risk of foreseeable harm.[74] The plaintiff must prove "the existence and amount of damages, based on actual harm of a legally recognized kind."[75] Courts apply the "but for" test to determine whether the defendant's conduct qualifies as a cause in fact.[76] A defendant proximately causes the plaintiff's injury when the harm occurs within a scope of risk created by the defendant's conduct, and the defendant's conduct makes the

---

subsequent robbery was foreseeable); Golombek v. Marine Midland Bank, N.A., 598 N.Y.S.2d 891, 892 (App. Div. 1993) (holding two prior incidents were insufficient to impose a duty). *But see* Taco Bell, Inc. v. Lannon, 744 P.2d 43, 48 (Colo. 1987) (holding ten armed robberies over three preceding years were sufficient to impose a duty); Nallan v. Helmsley-Spear Inc., 407 N.E.2d 451, 458 (N.Y. 1980) (holding 107 prior crimes on the property were sufficient to establish a duty). The Totality of the Circumstances Test imposes a duty when a crime becomes foreseeable based on all the circumstances including: "the nature, condition, and location of the premises, in addition to any prior similar incidents." *Boren*, 921 S.W.2d at 941. Under this approach a duty may exist even without a prior criminal attack of the same nature. *See, e.g.*, Issacs v. Huntington Mem'l Hosp., 695 P.2d 653, 661–62 (Cal. 1985) (imposing a duty on a hospital to protect patients from a doctor's assault as a result of being shot in the parking lot); Torres v. U.S. Nat'l Bank of Or., 670 P.2d 230, 235–36 (Or. Ct. App. 1983) (holding a duty existed to protect customers from foreseeable dangers while making a night deposit at the bank). For a discussion on tort liability for crimes committed by third parties at ATMs, see generally Chris A. Averitt, Note, *Bank Not Liable for Attack on ATM Patron:* Boren v. Worthen National Bank of Arkansas, 50 ARK. L. REV. 521 (1997) and Gregory W. Hoskins, Comment, *Violent Crimes at ATMs: Analysis of the Liability of Banks and the Regulation of Protective Measures*, 14 N. ILL. U. L. REV. 829 (1994).

[74] *See* DOBBS, HAYDEN & BUBLICK, *supra* note 71, § 159 ("What is foreseeable depends in large part on what facts the defendant actually knew or those he should have known, based on his obligation to know and act as a reasonable person."). No breach occurs with an adequately useful risk. *Id*. § 160. A foreseeable harm exists if the actor knew of the risk or a reasonable person in a similar position would recognize the risk. *Id*. § 159. Foreseeability alone fails to establish a breach of duty; the court must also weigh the probability that the conduct will inflict harm. Parsons v. Crown Disposal Co., 936 P.2d 70, 82 (Cal. 1997). A court may determine whether a risk is reasonable through a structured approach by weighing the risk of harm and utility of the defendant's conduct or by applying an unstructured balancing test weighing (1) the likelihood of the risk and (2) the amount of damage the risk will cause, against (3) the utility of the conduct and the cost of safety measures. *See* DOBBS, HAYDEN & BUBLICK, *supra* note 71, § 160–61 (explaining the structured and unstructured approaches to determining reasonableness).

[75] DOBBS, HAYDEN & BUBLICK, *supra* note 71, § 124. A legally recognized harm may be physical injury to person or property. *Id*.

[76] *Hale*, 166 S.W.3d at 718. Cause in fact does not mean sole cause; multiple causes in fact may exist. *Id*.; *see* McDonnell v. McPartlin, 736 N.E.2d 1074, 1080 (Ill. 2000) (stating that multiple parties causing an injury does not qualify as a defense to a negligence action). *But see* Guillot v. Sandoz, 497 So. 2d 753, 755–56 (La. Ct. App. 1986) (finding that a police department's failure to suspend a license was not a cause in fact because a suspension does not prevent a driver from continuing to drive); Ambrosio v. Carter's Shooting Ctr., Inc., 20 S.W.3d 262, 266 (Tex. App. 2000) (holding that a gun store's failure to exercise care in the storage and display of guns was not a cause in fact of the murder carried out with a gun stolen from the store because the connection was too attenuated).

harm foreseeable.[77] Besides using negligence to hold websites accountable, individuals may also bring claims of misrepresentation against websites.[78]

A plaintiff may sue for fraud, otherwise known as intentional misrepresentation, and negligent misrepresentation.[79] To establish a claim of fraud, a plaintiff must prove: (1) a representation of material fact; (2) falsely made; (3) with knowledge of its falsity; (4) with intent to defraud; (5) justifiable reliance upon the representation or concealment; and (6) an injury proximately caused by the reliance.[80] Similar to fraud, negligent misrepresentation requires: (1) representation of a material fact; (2) falsity; (3) justifiable reliance; and (4) damages proximately caused by the reliance.[81] Negligent misrepresentation replaces the intent and knowledge requirements with a proper relationship requirement.[82] Although some individuals allege claims of fraud and negligent

---

77 *See* DOBBS, HAYDEN & BUBLICK, *supra* note 71, § 198 ("To prevail in a negligence action, the plaintiff must bear the burden of showing that the harm she suffered is within the defendant's scope of liability . . . ."(footnote omitted)). A defendant's conduct does not qualify as a proximate cause if the harm is unforeseeable. *Id*. Multiple proximate causes may exist; therefore, multiple parties may sustain liability for the plaintiff's injuries. *Id*. However, a second actor or force may end the defendant's liability as a superseding cause. *Id*. The first actor's liability ends with an unforeseeable second act. *Id*.; *see id*. § 204 (discussing the difference between an intervening cause and a superseding cause); *see also* RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 34 cmt. b (2010) (defining intervening acts and superseding causes). Generally, the criminal act of a third party that causes the harm, which was not intended or foreseeable by the original negligent actor, breaks the causal chain of the original act. Annotation, *Intervening Criminal Act as Breaking Causal Chain*, 78 A.L.R. 471 (1932). However, the actor may remain negligent if a foreseeable criminal act of a third party occurs and involves an unreasonable risk of harm. RESTATEMENT (SECOND) OF TORTS § 302B (1965); *see id*. § 448 (defining when a criminal act fails to supersede a defendant's prior negligent act); *see also* Hines v. Garrett, 108 S.E. 690, 695 (Va. 1921) (stating that an actor remains liable when the alleged negligence exposes the injured party to the act causing the injury); RESTATEMENT (SECOND) OF TORTS § 449 (1965) (stating that an actor may incur liability for third-party criminal acts if the likelihood that someone may act criminally makes the actor's conduct negligent).

78 *See, e.g.*, Doe v. SexSearch.com, 502 F. Supp. 2d 719, 729 (N.D. Ohio 2007) (discussing plaintiff's fraud claim against website and the required elements for fraud), *aff'd*, 551 F.3d 412 (6th Cir. 2008); Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257, 1262 (N.D. Cal. 2006) (reviewing plaintiff's fraud and negligent misrepresentation claims against Yahoo!), *aff'd*, 376 Fed. App'x. 775 (9th Cir. 2010).

79 *See* Zitter, *supra* note 50, §§ 7, 20 (explaining the civil liability of online dating websites for actions involving negligent misrepresentation and fraud).

80 *See* DOBBS, HAYDEN & BUBLICK, *supra* note 71, § 664 (listing the requirements for an intentional misrepresentation or fraud claim); *see also* Zitter, *supra* note 50, § 20 (citing *Doe v. SexSearch.com* for the proposition that an individual may sue a dating website for fraud).

81 *See* MATTHEW A. CARTWRIGHT ET AL., LITIGATING BUSINESS AND COMMERCIAL TORT CASES § 3:7 (2011) (explaining the requirements of negligent misrepresentation).

82 *See id.* (recognizing that the requisite mental state differentiates fraud from negligent misrepresentation).

misrepresentation against online dating and social networking websites, this Note focuses solely on negligence actions.[83]

2. CDA Immunity: Social Networking and Online Dating Websites

Some victims attacked as a result of using social networking sites have sued the websites in hopes of holding the websites accountable for their injuries.[84] However, the courts—relying on the CDA—granted immunity to the websites.[85] For example, in *Carafano v. Metrosplash.com, Inc.*, the Ninth Circuit held Matchmaker.com, an online dating website, immune under the CDA.[86] Matchmaker.com allowed members to post profiles and view other members' profiles in their area.[87] An unknown person created a personal profile, imitating the plaintiff, which included lewd and sexual references.[88] Carafano sued the website for negligence,

---

83 *See infra* Part II.D.2 (explaining court decisions granting immunity to websites in negligence actions).

84 *See infra* note 85 (recognizing cases in which a plaintiff sued websites attempting to hold them accountable for their injuries).

85 *See, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008) (granting immunity under the CDA to a website faced with a negligence claim for failure to protect children from online predators); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 969–70 (N.D. Ill. 2009) (holding Craigslist immune under the CDA because third parties provided the content); Doe IX v. MySpace, Inc., 629 F. Supp. 2d 663, 665 (E.D. Tex. 2009) (finding MySpace immune under the CDA because users provided the information posted in their profiles); Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 298 (D.N.H. 2008) (holding an adult web community immune under the CDA because users provided the online personal ads).

86 339 F.3d 1119, 1125 (9th Cir. 2003). *But see* Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257, 1262–63 (N.D. Cal. 2006) (choosing not to grant immunity to a dating website from claims that it created fake profiles), *aff'd*, 376 Fed. App'x. 775 (9th Cir. 2010). *See generally* Jeffrey Lipschutz, Case Note, *Internet Dating . . . Not Much Protection Provided by the Communications Decency Act of 1996 Based on* Carafano v. Metrosplash.com*, 339 F.3d 1119 (9th Cir. 2003)*, 23 TEMP. ENVTL. L. & TECH. J. 225 (2004) (providing a case study of *Carafano*). Anthony's claim that Yahoo! created fake profiles treated Yahoo! as an ICP because Anthony alleged Yahoo! created the content. *Anthony*, 421 F. Supp. 2d at 1262–63. However, the CDA failed to grant Yahoo! immunity because only ICS's are treated as a publisher of third-party content and receive immunity, rather than content providers. *Id.*

87 *Carafano*, 339 F.3d at 1121. The profiles usually contained a few pictures, descriptive information about the member, and answers to questions that portrayed the member's personality. *Id.* Matchmaker.com required members to complete a questionnaire with over fifty questions to fill the content of their profile. *Id.* Matchmaker.com created the questionnaire and provided answers users could select from when completing the questionnaire. Lipschutz, *supra* note 86, at 227.

88 *Carafano*, 339 F.3d at 1121. The profile indicated the member was looking for a one-night stand and gave other indications of sexual behavior. *Id.* The profile also sent an email containing the plaintiff's home address and telephone number to anyone that sent a message to the profile. *Id.* Matchmaker.com's policy prohibited members from including last names, addresses, phone numbers, or other personal contact information within the profiles. Lipschutz, *supra* note 86, at 228. However, Matchmaker.com relied on users to report inappropriate profile information, and once informed, Matchmaker.com either

invasion of privacy, and defamation, but the court granted immunity to the website because third parties primarily provided the information.[89] The court granted Matchmaker.com immunity as an ICS because the profiles only existed or contained content once users created them, and a third party created the information within the relevant profile that led to the harm.[90]

In addition to granting immunity to a dating website, the CDA allows social networking sites to claim immunity from tort actions.[91] For instance, in *Doe v. MySpace, Inc.*, a thirteen-year-old girl created a

---

edited or deleted the profile. *Id.* The profile led to Carafano receiving obscene, sexually explicit communications and a fax threatening her son. *Id*. at 229. An unknown person in Europe created the profile on October 23, 1999. *Id.* at 228. Carafano later learned of the profile and notified police on November 5, 1999. *Id.* at 229. Carafano's manager also notified Matchmaker.com on November 6, 1999, which caused Matchmaker.com to delete the profile on November 9, 1999. *Id*.

89 *Carafano*, 339 F.3d at 1122, 1125. The court granted Matchmaker.com immunity because it "did not play a significant role in creating, developing, or 'transforming' the relevant information." *Id*. at 1125; *see* John E. D. Larkin, *Criminal and Civil Liability for User Generated Content: Craigslist, a Case Study*, 15 J. TECH. L. & POL'Y 85, 107 (2010) (discussing how Matchmaker.com provided questions that users answered for dating matches, which resulted in Matchmaker.com's ICP declaration).

90 *Carafano*, 339 F.3d at 1124–25. The court viewed Matchmaker.com as an ICS even though it provided questions to assist with completing the profile because third parties supplied the answers and users chose the content. *Id*. at 1124; *see* Green v. Am. Online, 318 F.3d 465, 470–71 (3d Cir. 2003) (barring an argument for failure to protect a user because third parties provided the content); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 714–16 (Ct. App. 2002) (barring a negligence claim against eBay due to the CDA because the content provided was created by third parties). *But see* Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 802 (N.D. Cal. 2011) (denying immunity under the CDA in an unlawful misappropriation action). In *Fraley v. Facebook, Inc.*, the court rejected Facebook's CDA immunity argument because the plaintiffs claimed Facebook used information provided by users to create new content published as endorsements. *Id*. at 801. Although the court agreed with Facebook regarding its ICS status, the court relied on *Roommates.com*'s reasoning to define Facebook as both an ICS and ICP. *Id*. at 801–02.

91 *See, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008) (granting a website immunity under the CDA in a negligence claim for failure to protect children from online predators); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 968–70 (N.D. Ill. 2009) (holding Craigslist immune under the CDA because the content is provided by third parties); Doe IX v. MySpace, Inc., 629 F. Supp. 2d 663, 665 (E.D. Tex. 2009) (finding MySpace immune under the CDA because users provide the information posted in their profiles); Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 298 (D.N.H. 2008) (granting an adult web community immunity under the CDA because users provided the online personal ads). *But see* Matthew Altenberg, Comment, *Playing the Mysterious Game of Online Love: Examining an Emerging Trend of Limiting § 230 Immunity of the Communications Decency Act and the Effects on E-Dating Websites*, 32 PACE L. REV. 922, 948–51 (2012) (arguing that the current trend of courts makes a narrower application of the CDA possible, which may allow individuals to hold dating websites liable).

MySpace profile representing herself as eighteen years old.[92] The profile allowed nineteen-year-old Pete Solis to contact Doe, and the two began communicating offline via telephone.[93] However, once they met in person, Solis sexually assaulted Doe.[94] Doe's mother sued MySpace alleging it failed to utilize proper safety measures to prevent predators from contacting minors online.[95] The Does filed claims for negligence, gross negligence, fraud, and negligent misrepresentation against MySpace.[96] The court barred the claims via the CDA because the Does' failure-to-protect argument merely rephrased a claim that attempted to hold MySpace liable for publishing third-party content.[97]

---

92 528 F.3d at 416. MySpace admitted users fourteen or older, and the website automatically set the profiles of members under sixteen to "private," limiting the information others could view. *Id*. *See generally* Sarah Merritt, Comment, *Sex, Lies, and MySpace*, 18 ALB. L.J. SCI. & TECH. 593 (2008) (discussing the dangers of MySpace and how to prevent the sexual assaults and predators on the internet); Norby-Jahner, *supra* note 49, at 208–09 (explaining how predators sexually harass minors online and describing that victims share a limited legal remedy for their harm); Elizabeth P. Stedman, Comment, *MySpace, but Whose Responsibility? Liability of Social-Networking Websites When Offline Sexual Assault of Minors Follows Online Interaction*, 14 VILL. SPORTS & ENT. L.J. 363 (2007) (assessing the liability of social networking websites when predators sexually assault minors offline).

93 *Doe*, 528 F.3d at 416.

94 *Id*. Doe volunteered her phone number to communicate with Solis, and the sexual assault took place within one month of Solis's initial online contact. *Id*. Following *Doe v. MySpace*, MySpace made agreements to increase online safety. Chelsea Peters, Comment, *MySpace or Yours? The Impact of the MySpace-Attorneys General Agreement on Online Businesses*, 5 SHIDLER J.L. COM. & TECH. 10, 2–6 (2008), *available at* digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/424/1015_no2_art10.pdf?sequence=1 (discussing MySpace's agreement regarding goals to improve online safety for minors). The agreement included four categories to improve safety: (1) online safety tools; (2) design and functionality changes; (3) education for parents, educators, and children; and (4) law enforcement cooperation. *Id*.

95 *Doe*, 528 F.3d at 416; *see* Merritt, *supra* note 92, at 621–24 (suggesting Congress should create a national ID system for individuals to access the Internet to protect children online); Stedman, *supra* note 92, at 397 (suggesting that MySpace implement an age verification system by requiring credit cards to create a profile); *see also* Sharon Nelson et al., *The Legal Implications of Social Networking*, 22 REGENT U. L. REV. 1, 23–26 (2009) (discussing the dangers of sexual predators on social networking sites); Krista L. Blaisdell, Note, *Protecting the Playgrounds of the Twenty-First Century: Analyzing Computer and Internet Restrictions for Internet Sex Offenders*, 43 VAL. U. L. REV. 1155, 1204–08 (2009) (proposing a model state statute that limits and restricts computer and Internet use for released sex offenders).

96 *Doe*, 528 F.3d at 416.

97 *Id*. at 419–20. The court further characterized Doe's argument as holding MySpace liable because Doe lied about her age, Doe disregarded MySpace's safety recommendations, and the parents allowed Doe to create a profile; although, MySpace knew of the risk that users could lie. *Id*. at 421–22. Additionally, the district court rejected the argument, viewing it as "artful pleading," to hold MySpace liable for publishing communications between Doe and Solis. *Id*. at 419–20; *see* Green v. Am. Online, 318 F.3d 465, 469–70 (3d Cir. 2003) (rejecting plaintiffs' failure-to-protect argument after re-characterizing the claim as holding AOL liable for failing to screen third-party content). In

Although courts continue to rely on the CDA to grant immunity to websites, many critics disagree with this policy and ultimately proposed solutions to reduce immunity.[98] In addition, even though courts grant immunity to websites under the CDA, which prevents victims from holding websites accountable, criminal background checks may help reduce the number of attacks.[99]

Green v. America Online, the plaintiff sued AOL after receiving a computer virus and receiving derogatory comments in a chat room. *Id*. The plaintiff based his failure-to-protect argument on AOL's Community Guidelines that outlined standards for online speech and conduct. *Id*; *see* Doe v. SexSearch.com, 502 F. Supp. 2d 719, 727–28 (N.D. Ohio 2007) (granting immunity to the website when plaintiff claimed the website failed to prevent minors from using the site), *aff'd*, 551 F.3d 412 (6th Cir. 2008). In *Doe v. SexSearch.com*, SexSearch.com—an adult dating service—helped users connect for sexual encounters; however, Doe, a member of the service, connected with a minor via the website and eventually received criminal charges. *Id*. at 722. The court granted immunity, determining the plaintiff attempted to plead around the CDA to hold the website accountable for publishing the minor's profile. *Id*. at 727–28. Although the court granted the website immunity from plaintiff's tort claims, the court further held that the CDA grants immunity from all civil liability. *Id*.

98 *See* Gray, *supra* note 49, at 421 (suggesting an amendment to the CDA would prevent courts from granting online dating websites immunity for failing to protect their users from fraud); Lipschutz, *supra* note 86, at 241 (proposing a balancing test to determine CDA immunity); Norby-Jahner, *supra* note 49, at 259–60 (proposing an amendment to the CDA to create liability for social networking sites); Lisa Marie Ross, Note, *Cyberspace: The New Frontier for Housing Discrimination—An Analysis of the Conflict Between the Communications Decency Act and the Fair Housing Act*, 44 VAL. U. L. REV. 329, 374–75 (2009) (amending the CDA to remove exceptions and incorporate a clause that limits the CDA's application to instances included within the CDA's text); Seaton, *supra* note 57, at 375 (suggesting a new test for CDA immunity that considers the collective effect of the ICS, the claim at issue, and the alleged facts of the case); Daniel Zharkovsky, Note, *"If Man Will Strike, Strike Through the Mask": Striking Through Section 230 Defenses Using the Tort of Intentional Infliction of Emotional Distress*, 44 COLUM. J.L. & SOC. PROBS. 193, 231–32 (2010) (proposing the law should hold websites liable for their users' torts of intentional infliction of emotional distress); *see also* Ashley Ingber, Note, *Cyber Crime Control: Will Websites Ever Be Held Accountable for the Legal Activities They Profit From?*, 18 CARDOZO J.L. & GENDER 423, 447 (2012) (concluding the CDA may not grant websites immunity from criminal charges). *But see* Walters, *supra* note 28, at 211–12 (claiming that websites should be granted immunity from claims involving a third-party criminal actor utilizing the website to perform criminal activity); Ryan French, Comment, *Picking up the Pieces: Finding Unity After the Communications Decency Act Section 230 Jurisprudential Clash*, 72 LA. L. REV. 443, 485 (2012) (concluding that the *Zeran* approach of broad immunity best interprets the CDA and suggesting all courts adopt that reasoning to provide uniformity); Matthew Schruers, Note, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 206–08 (2002) (analyzing how the current state of the law provides the most economic efficiency for websites); Ziniti, *supra* note 55, at 594 (arguing that the *Zeran* approach to granting broad immunity is better than alternatives granting less immunity).

99 *See infra* Part II.E (discussing criminal background checks and online dating).

E. Criminal Background Checks

Criminal background checks allow someone to access an individual's prior criminal convictions including felonies, misdemeanors, or other possible offenses.[100] This section explains the scope, cost, and drawbacks of criminal background checks.[101] Criminal background checks provide criminal records from federal, national, and county databases.[102] Many providers offer a national criminal background check that includes records from all available databases.[103] The cost of a single criminal background check varies depending on the provider.[104] Intelius offers a single national check for $39.95, Sentry Link offers a fifty-state check for $19.95, and U.S. Criminal Checks, Inc. offers a $12.95 nationwide check.[105] Many providers also offer a volume or

---

100 *See Criminal Records*, INTELIUS, https://www.intelius.com/criminal-check.html (last visited Aug. 10, 2013) (stating a criminal report includes criminal convictions such as felonies, misdemeanors, and other criminal offenses); *National Criminal Background Checks*, CRIM. BACKGROUND RECS., http://www.criminalbackgroundrecords.com/national-criminal-background-check.html (last visited Aug. 10, 2013) (offering records for felonies, misdemeanors, and lesser criminal offense convictions and checks against the sex offender and most wanted lists); *What Is and Isn't Revealed Through a Background Check?*, BACKGROUNDCHECK.ORG, http://www.backgroundcheck.org/basics/what-is-and-isnt-revealed-through-a-background-check/ (last visited Aug. 10, 2013) (discussing what someone may access via a criminal background check). Additionally, depending on the scope of the search, the check may reveal arrest and incarceration records or outstanding warrants. *Id*.

101 *See infra* notes 102–11 and accompanying text (discussing the scope, expense, and inadequacies of criminal background checks).

102 *What Is and Isn't Revealed Through a Background Check?*, *supra* note 100.

103 *See, e.g.*, *Criminal Records*, *supra* note 100 (offering a single national background check); *National Criminal Background Checks*, *supra* note 100 (including records from federal, state, and county databases in the background check); *Nationwide Criminal Background Searches*, U.S. CRIMINAL CHECKS, INC., https://www.criminalcbs.com (last visited Aug. 10, 2013) (providing federal, state, and county records within one nationwide search). *But see National Criminal Background Check & Sex Offender Check*, SENTRYLINK, http://www.sentrylink.com/web/loadCriminalReport.do (last visited Aug. 10, 2013) (failing to provide federal records within a national criminal background check).

104 *See infra* note 105 and accompanying text (discussing the prices associated with criminal background checks from various providers).

105 *Get the Information You Need on John Doe*, INTELIUS, https://www.intelius.com (last visited Sept. 12, 2013) (search "People Search" for "John Doe"; then follow "Get the report on" for the first match) (pricing a single Intelius national criminal background check at $39.95); *National Criminal Background Check & Sex Offender Check*, *supra* note 103 (offering a fifty-state check for $19.95); *Nationwide Criminal Background Searches*, *supra* note 103 (selling a $12.95 nationwide criminal records check); *see National Criminal Background Checks*, *supra* note 100 (listing a $59.95 price for a single national criminal background check); *see also* Mandy Stadtmiller, *Check Mate—More Women Paying to Investigate Dates; Before Dinner, a Background Check*, N.Y. POST, Sept. 27, 2006, at 39, *available at* 2006 WLNR 16758576 (discussing that people pay for criminal background checks before meeting someone from a dating website).

corporate discount, which generates a lower price per check for large orders.[106] Although many websites offer criminal background checks, the online dating industry believes criminal background checks will not increase safety.[107]

The dating website industry believes the cost of requiring criminal background checks outweighs the benefits.[108] The industry also contends that requiring background checks will reduce the privacy of users and may reduce the amount of self-checking that users perform before meeting another user.[109] Thus, industry leaders advocate for increasing the promotion of safety guidelines to improve safety, rather than relying on background checks that are not 100% accurate.[110] Although online dating websites oppose criminal background checks, other industries believe criminal background checks will provide safety benefits.[111] Therefore, Part III analyzes whether requiring criminal background checks for dating websites will improve user safety.[112]

---

106 *See Nationwide Criminal Background Searches*, *supra* note 103 (allowing corporate accounts a discount); *Search More & Pay Less with Volume Discount Packages*, INTELIUS, https://www.intelius.com/salescontact.php (last visited Sept. 12, 2013) (offering a volume discount for large orders).

107 *See* Ken Greenberg, *In Wake of Major Security Breaches at Data Providers, Dating Site/Social Networking Trade Group Announces Opposition to State Legislation Aimed at Regulating Online Dating*, BUS. WIRE (Mar. 21, 2005, 9:01 AM), http://www.businesswire.com/news/home/20050321005474/en/Wake-Major-Security-Breaches-Data-Providers-Dating (discussing why dating websites oppose requiring criminal background checks).

108 *See id*. (arguing that online users may screen their dates; therefore, meeting online is already safer than meeting someone at a bar). For example, the industry believes criminal background checks will create a "false sense of security." *Id*.; *see supra* note 40 (discussing the Internet Alliance's belief that criminal background checks will mistakenly provide users with an increased belief in user safety online). *But see* Maureen Horcher, Comment, *World Wide Web of Love, Lies, and Legislation: Why Online Dating Websites Should Screen Members*, 29 J. MARSHALL J. COMPUTER & INFO. L. 251, 276–77 (2011) (arguing for federal legislation that requires fee-charging dating websites to perform criminal background checks on users).

109 Greenberg, *supra* note 107 (outlining the comments of online dating industry leaders who oppose a criminal background check requirement). *But see supra* note 27 (providing examples of the risks faced by users of online dating websites that fail to conduct criminal background checks).

110 Greenberg, *supra* note 107 (stating industry leaders want to maintain the current safety measures). Additionally, opponents of background checks suggest the solution will only provide substantial money to background check providers without solving the problem. *Id*.; *see supra* notes 27, 40–41 (explaining the safety measures that current dating websites suggest to prevent dangerous encounters and discussing how state statutes requiring that dating websites notify users whether they perform criminal background checks have added additional requirements to provide awareness about criminal background checks).

111 *See* Jon E. Anderson & M. Scott LeBlanc, *Skeletons in the Closet? Minimizing the Risks of Background Checking*, 85 WIS. LAW., Sept. 2012, at 12, 12–13 (explaining how employers use background checks to identify dangerous job applicants and to verify the information

III. ANALYSIS

Part III assesses the current state of the law regarding online dating websites and considers the impact that criminal background checks may have on the online dating industry.[113] Part III.A examines current state statutes and analyzes how the statutes inadequately protect users.[114] Next, Part III.B evaluates the Internet's evolution and proposes that the Internet's increasing importance should alter how courts determine a website's liability.[115] Part III.B.1 assesses the strengths and weaknesses of the courts' reliance on decisions dating back to the CDA's origin.[116] Part III.B.2 analyzes current CDA immunity law and how it affects the users of online dating websites.[117] Last, Part III.C demonstrates the effects and feasibility of implementing background checks into a dating website's safety procedures.[118]

A. State Statutes: Assessing the Current Protections for Online Dating Users

Aware of the dangers involved with online dating, states enacted statutes to regulate dating websites and protect users' safety.[119] The

---

provided by the applicant); Barbara A. Lee, *Who Are You? Fraudulent Credentials and Background Checks in Academe*, 32 J.C. & U.L. 655, 656–57 (2006) (discussing the use of background checks for teachers, university faculty members, and other employees that work with children); *To Curb Gun Violence, Enact Universal Background Checks*, USA TODAY, Feb. 11, 2013, at 8A, *available at* 2013 WLNR 3409950 (suggesting mandatory background checks on gun purchasers to reduce gun violence).

112 *See infra* Part III.C.1 (assessing whether criminal background checks will improve online daters' safety).

113 *See infra* Parts III.A, C (providing an overview of the effectiveness of current state statutes designed to protect dating website users and comparing the strengths and weaknesses of requiring dating websites to perform criminal background checks).

114 *See infra* Part III.A (considering the current solutions states have implemented to protect users of online dating websites).

115 *See infra* Part III.B.1 (discussing how the impact of the Internet within society should force courts to revise their outlook on website liability).

116 *See infra* Part III.B.1 (describing how courts should alter their decisions on CDA immunity to coincide with the Internet evolution).

117 *See infra* Part III.B.2 (assessing the current state of CDA immunity decisions and how these decisions fail to provide relief for victims involved in criminal attacks stemming from online connections).

118 *See infra* Part III.C (explaining how criminal background checks will increase the safety of using online dating websites and arguing that the online dating industry can financially withstand a requirement to perform criminal background checks on users).

119 *E.g.*, ARIZ. REV. STAT. ANN. §§ 44-7152 to -7154 (West, WestlawNext through legislation effective June 20, 2013 of the 1st Reg. Sess. of the 51st Leg.) (regulating how an online dating website may contract with its users); N.J. STAT. ANN. §§ 56:8-169 to -173 (West, WestlawNext through L.2013, c. 84 and J.R. No. 9) (requiring dating websites to notify users whether the website performs criminal background checks); *see supra* Part II.B (discussing state statutes affecting online dating websites and users).

majority of the statutes solely affect the interactions between dating websites and their users; therefore, the statutes fail to protect users from other harmful, even criminal, individuals who use the dating websites.[120] Although some states designed their statutes to enhance the safety of users on dating websites, the statutes only bring awareness to the problem and fail to implement a solution.[121] The statutes require dating websites to notify users whether the website conducts criminal background checks, which educates users about the possible dangers, but only increases safety through an individual's own actions.[122] Furthermore, the major dating websites implemented notifications complying with New Jersey's statute.[123] Such notifications helped increase the users' awareness about possible criminal attacks stemming from online dating, but failed to prevent or lessen recent attacks.[124]

---

120 *See* Coleman, *supra* note 34, at 144–57 (providing an overview of state statutes affecting dating websites and discussing how only New Jersey enacted a statute to protect users from dangers beyond dating services); *see also, e.g.*, CAL. CIV. CODE § 1694.2 (West, WestlawNext current with urgency legislation through ch. 70 of 2013 Reg. Sess.) (requiring that dating websites: (1) provide users with a copy of the contract; (2) institute specific statements regarding the cancellation of the user's contract; and (3) implement a three business day rescission period for users to void the contract); N.Y. GEN. BUS. LAW § 394-c (McKinney, WestlawNext through L.2013, chapters 1 to 57 and 60 to 110) (limiting fees to $1000 annually, requiring sellers who charge more than $25 monthly to provide a set number of referrals per month, and allowing users to cancel their contract and receive a refund if the seller fails to provide the required number of referrals for two or more consecutive months).

121 *See* N.J. STAT. ANN. § 56:8-171 (mandating that dating services notify users: (1) that one should take reasonable precautions to protect oneself when using the service; (2) that criminal background checks fail to screen all users; (3) that users should not believe in absolute security of criminal background checks; (4) that the service does or does not conduct criminal background checks; and (5) that the service does or does not allow members with known criminal backgrounds to join the website); *see also* Coleman, *supra* note 34, at 149–50 (reviewing arguments in favor of and against New Jersey's statute that requires dating sites to notify users whether they conduct criminal background checks); Lade, *supra* note 39 (discussing Representative Kevin Ambler's attempts to sponsor a similar statute in Florida). Parties disfavoring criminal background checks believe such a requirement may create additional dangers by providing "a false sense of security." *Id.*

122 Coleman, *supra* note 34, at 150 (discussing that individuals may follow safety tips provided by the website or conduct their own investigation of users to ensure their safety); *see supra* note 27 (overviewing the safety tips that major dating sites recommend users follow to ensure online dating safety).

123 *See supra* note 25 (explaining how major dating sites Match.com and eHarmony notify users that neither site performs criminal background checks on users)

124 *See supra* notes 28–29 (listing recent criminal attacks on users of dating websites by their referred date); *see also supra* note 27 (stating the safety precautions dating websites recommend to their users to increase safety).

In addition to complying with New Jersey's statute, dating websites implemented their own safety measures.[125] Dating websites recommend users follow dating safety tips to ensure safety online and safety when meeting someone new offline.[126] Yet, similar to the New Jersey statute, the recommendations only improve safety through an individual's own precautions.[127] Furthermore, many women pay for criminal background checks on users before meeting them, rather than simply relying on the recommended safety precautions.[128] In doing so, the users realize dangers exist and understand that solely relying on the dating website's recommendations may not provide adequate security.[129] Unfortunately, increased awareness about the possible dangers and recommended safety precautions failed to curtail attacks resulting from online dating.[130] However, victims also face an additional problem, current CDA law grants websites immunity from negligence claims.[131]

B. Evolution of the Internet and CDA Immunity

In recent years, the Internet has evolved to capsulate how individuals communicate, receive information, and perform many other daily tasks.[132] However, courts continue to rely on case law that protected dating websites before the Internet evolution.[133] Part III.B.1 assesses whether courts should maintain their current line of reasoning regarding CDA immunity even though the Internet has evolved since the

---

125 *See supra* note 27 (discussing the safety recommendations that dating websites provide to users).

126 *See supra* note 41 (listing the statute's recommended safety measures including: (1) notify a third party when meeting someone new; (2) meet in a public place; (3) provide your own transportation; and (4) refuse to provide personal contact information beyond the website profile).

127 *See supra* note 41 (recognizing that an individual user must take affirmative steps to utilize these precautions); *see also* Stadtmiller, *supra* note 105 (explaining that many women pay for their own criminal background checks before meeting someone from a dating website).

128 *See* Stadtmiller, *supra* note 105 (noticing the trend of users performing their own criminal background checks to improve their safety with online dating).

129 *See id.* (pointing out that one private investigator believes dating website users lie 50% of the time, making criminal background checks necessary).

130 *See supra* text accompanying note 124 (identifying that the notifications provided by dating websites did not decrease the number of attacks on users).

131 *See infra* Part III.B.2 (analyzing why the current interpretation of CDA immunity fails to hold websites accountable for placing individuals into dangerous situations).

132 *See supra* Part II.A (discussing the evolution of the internet and its influence on society's daily lives).

133 *See supra* Part II.C (providing an overview of cases decided under the purview of the CDA that have granted websites immunity from negligence claims).

CDA's enactment.[134] Part III.B.2 analyzes whether the CDA should provide victims of a criminal attack, stemming from online dating, an opportunity to hold the website accountable for the attack.[135]

1. Outdated Precedent Guides CDA Court Decisions

While the courts' initial reasoning protected websites with unknown capabilities and potential, continuing to rely on outdated precedent unfairly protects large, successful businesses over individuals.[136] Therefore, rather than continuing to grant websites a broad range of immunity from tort claims, courts should treat websites similar to brick and mortar stores when deciding liability.[137] Although treating websites similar to brick and mortar stores contradicts the original intent of the CDA, such reasoning provides victims with an opportunity to hold websites accountable for placing individuals into harmful situations involving possible criminal attacks.[138]

---

134 *See infra* Part III.B.1 (analyzing the strengths and weaknesses of current court decisions that invoke CDA immunity reasoning despite the increased use of the Internet).

135 *See infra* Part III.B.2 (arguing that the CDA should impose liability on dating websites for failing to protect users from possible criminal attacks).

136 *See, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008) (using the CDA to hold MySpace—a successful social networking site—immune from a negligence action brought by a user); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 969 (N.D. Ill. 2009) (granting Craigslist immunity under the CDA from tort actions); *supra* notes 60–64 (discussing the growth of the internet and the increase in earnings and profits of large Internet-based companies); *see also* Horcher, *supra* note 108, at 266–68 (arguing that courts rely on outdated policy when upholding the CDA). The current CDA policy fails to consider that the Internet provides numerous services and has evolved into a dominant channel for commerce. *Id*. at 267.

137 *See supra* note 73 (explaining the tests courts use to determine the liability of a store that places its customers into a dangerous situation). Courts apply one of three tests to determine whether a duty exists to protect individuals or customers from the criminal acts of third parties. Boren v. Worthen Nat'l Bank of Ark., 921 S.W.2d 934, 940 (Ark. 1996); *see supra* note 73 (examining the factors and circumstances courts use when applying these tests and discussing cases where courts decided whether or not a legal duty existed).

138 *See* Stedman, *supra* note 92, at 391–92 (arguing that social networking sites should face liability for failing to protect children from online predators). Stedman's solution requires MySpace to verify users' ages through credit card numbers; therefore, parents know about their child's account and may limit who their child may interact with online through age restrictions. *Id*. at 397. Stedman states MySpace's failure to implement an age verification system was negligent and thus, courts should find MySpace liable for allowing children to interact with dangerous adults online. *Id*. at 391–92; *see* Merritt, *supra* note 92, at 621–24 (concluding that the current law prevents victims from holding MySpace liable when children interact with online predators and proposing an age verification system to protect children online).

Proponents of the CDA mistakenly believe that the courts' current reasoning best supports how society uses the Internet today.[139] Supporters argue websites need immunity to continue to innovate because websites use information provided by third parties to create more value for users.[140] However, proponents of the CDA argue this perspective only in regard to the posting of defamatory content, rather than assessing the impact that the current approach imposes on negligence claims against websites.[141] Furthermore, the current scheme allows websites to provide more value because websites remain unaccountable for failing to protect their users from online and offline dangers.[142] The current reasoning adopted by courts unfairly protects websites over victims; more specifically, the current reasoning unfairly

---

139 *See* Schruers, *supra* note 98, at 206–08 (arguing that the current state of the law provides the most economic efficiency for websites); Ziniti, *supra* note 55, at 594 (reasoning that limiting website immunity will destroy the significant value created by interactive websites). *But see* Gray, *supra* note 49, at 426 (stating that the current law leaves the website immune from liability and the original culpable party fails to receive punishment); *see, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997) (holding the website immune; thus, preventing the victim from recovering damages). In *Zeran v. AOL*, the original party responsible for posting the content never received due punishment. *Id.* at 329.

140 Ziniti, *supra* note 55, at 594 (stating websites that provide value through the content of others—including Wikipedia or Google—would significantly reduce the value they provide due to increased liability). Ziniti assesses different alternatives to the *Zeran* approach and ultimately concludes that the benefits of the *Zeran* approach provides the best situation for search engines, traditional websites, content distributors, and content-based advertising online. *Id.* at 610–14; *see* Schruers, *supra* note 98, at 256–60 (claiming that a non-liability approach most efficiently regulates the economics of ISPs because liability fails to deter ISPs). Schruers deems the tort behavior unavoidable; therefore, ISPs cannot prevent the torts and liability would not deter the ISPs. *Id.* at 260. *But see* Gray, *supra* note 49, at 416–17 (arguing that protecting websites that allow third parties to post fraudulent information fails to spark innovation and suppresses fundamental rights).

141 *See* Schruers, *supra* note 98, at 208 (reviewing the economic impact of different liability schemes regarding the monitoring of third-party content). *But see* Seaton, *supra* note 57, at 375–77 (arguing the current approach ineffectively determines liability and suggesting that courts should consider the nature of the ICS, the type of claim, and the facts alleged when determining liability). *See generally* Ziniti, *supra* note 55 (assessing why the *Zeran* approach most effectively determines liability for websites that regulate third-party content).

142 *See, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008) (granting MySpace immunity from liability, even though the facts alleged that MySpace failed to protect minor users from adult predators); *supra* note 91 (discussing cases granting immunity under the CDA to websites for failing to protect their users from dangers online and offline); *see also supra* note 95 (listing proposed solutions to the CDA immunity problem that create methods for holding websites accountable for failing to protect their users). Additionally, dating websites earn increased profits and increased sales; therefore, the industry can withstand increased liability. *See* Gray, *supra* note 49, at 417 (providing that online dating websites can afford to monitor users due to their excessive profits).

affects the victims of criminal attacks stemming from an online dating website's failure to perform a criminal background check.[143]

2. CDA Immunity and Online Dating Websites

Currently the CDA bars negligence actions against websites.[144] This unfairly restricts victims from holding dating websites accountable for failing to perform criminal background checks on users.[145] Someone attacked as a result of a dating website's failure to perform criminal background checks may establish each element of a negligence claim except duty.[146] Yet, courts grant immunity to websites before hearing the merits of a victim's case.[147] Therefore, the CDA denies a victim the opportunity to hold a website accountable for its actions even though a victim may establish four of the five required elements for negligence.[148]

---

143 *See infra* Part III.B.2 (assessing the impact of CDA immunity granted to websites in negligence actions that are brought against a dating website for failing to perform criminal background checks).

144 *See, e.g.*, *Doe*, 528 F.3d at 422 (holding MySpace immune under the CDA from a negligence cause of action); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 969 (N.D. Ill. 2009) (granting Craigslist immunity under the CDA from a negligence suit); Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 298 (D.N.H. 2008) (finding a social networking website immune from a negligence claim); *see also supra* Part II.D.2 (discussing the CDA and decisions granting websites immunity thereunder).

145 *See* Lipschutz, *supra* note 86, at 239 (stating the court decision in *Carafano* unfairly granted immunity to a dating website). Lipschutz argues that the *Carafano* decision unfairly protects websites because the same action distributed through a book or television broadcast would create liability. *Id*. He further argues that Matchmaker.com was liable because the website charges users a fee and, as a business, maintains a duty to protect customers while using the service. *Id*. at 240.

146 *See, e.g.*, *Doe*, 528 F.3d at 422 (dismissing a negligence claim against MySpace under the CDA without deciding whether MySpace negligently failed to protect the minor victim from sexual predators).

147 *See supra* Part II.D (discussing the requirements and outcomes of tort actions brought against online dating and social networking websites); *supra* notes 85, 91 and accompanying text (illustrating that court decisions unfairly dismiss negligence actions against websites under the CDA before hearing any of the arguments on the merits). *See generally* Zitter, *supra* note 50 (discussing cases where courts granted a defendant's motion to dismiss because websites received immunity under the CDA).

148 *See* Merritt, *supra* note 92, at 602 (stating victims without a widespread remedy need to sue to force change). Merritt suggests parents need to sue MySpace for failing to protect their children online to receive compensation or to force MySpace to better protect their users online and offline. *Id*. *But see* Stedman, *supra* note 92, at 391–92 (concluding MySpace acted negligently by failing to protect children from online sexual predators). Stedman contends that the CDA's policy supports the determination that MySpace was not the proximate cause of the victim's injuries. *Id*. at 390

Additionally, by barring negligence suits, courts expanded the CDA beyond its original purpose.[149] Congress enacted the CDA to allow websites to regulate third-party content posted on its pages without imposing liability for publishing information; however, court decisions expanded the CDA's grant of immunity beyond its intended scope.[150] In doing so, courts unfairly granted websites immunity in negligence actions when Congress did not intend for such a result.[151] Courts misinterpreted the CDA and ultimately barred victims from holding websites accountable by granting websites immunity from negligence actions under the CDA.[152] For a victim to ultimately succeed in a negligence suit and hold a website accountable for its actions, the law must impose a duty on dating websites to perform criminal background checks.[153]

C. Criminal Background Checks and Dating Websites

In recent years, criminal background checks became more effective, and now many employers and schools use checks to screen for possible dangers.[154] However, dating websites fail to incorporate criminal background checks into their safety procedures to protect users.[155] Part III.C.1 assesses whether criminal background checks will reduce the dangers associated with online dating.[156] Part III.C.2 analyzes whether

---

149 *See supra* Part II.C.1 (explaining Congress's original intent for enacting the CDA); *see also* Cannon, *supra* note 44, at 52–53 (identifying the original purpose of the CDA was to limit the exposure of pornography to children on the Internet).

150 *See* Ottenweller, *supra* note 48, at 1303–04 (discussing Congress's original intent for passing the CDA); *supra* notes 90–91, 97 (explaining court decisions that granted immunity to websites for all tort claims rather than solely for claims regarding free speech on the Internet).

151 *See, e.g.*, *Doe*, 528 F.3d at 422 (granting a website immunity in a negligence action by invoking the CDA); *see supra* notes 90–91 (discussing instances where courts granted immunity under the CDA beyond the CDA's original intended scope).

152 *See* Ottenweller, *supra* note 48, at 1310–12 (arguing that courts misinterpreted the CDA and granted negligent websites "get out of jail free" cards).

153 *See infra* Part III.C (analyzing whether requiring dating websites to perform criminal background checks will increase users' safety and whether imposing a duty to perform criminal background checks will allow dating websites to remain profitable).

154 *See supra* Part II.E (discussing criminal background checks and their increase in popularity to effectively screen for possible dangers).

155 *See supra* Part II.A (reviewing the current safety methods and procedures dating websites use to protect or increase the safety of using their services).

156 *See infra* Part III.C.1 (determining how effectively criminal background checks may screen for possible dangerous users of online dating websites).

dating websites can withstand the expense of performing criminal background checks on users.[157]

1. Criminal Background Checks Will Reduce the Dangers of Online Dating

Despite the possibility that criminal background checks may improve the safety of online dating, online dating websites fail to implement criminal background checks into their safety procedures.[158] Online criminal background checks contain nationwide records allowing checks of federal, state, and county criminal records; therefore, dating websites may efficiently determine—with one quick search—whether a user previously committed a dangerous crime.[159] However, some drawbacks in implementing criminal background checks exist including: (1) the checks may not catch all users with criminal backgrounds; (2) the checks fail to flag predators without a prior conviction or arrest; and (3) many false profiles exist or predators may create false profiles to circumvent the background checks.[160] Nevertheless, background checks will still flag some dangerous individuals online, which will help prevent possible dangerous encounters.[161]

Additionally, opponents in favor of requiring that dating websites perform background checks believe mandating background checks will provide a false sense of security for users.[162] Yet, the notifications provided to users, regarding their recommended date's criminal background, may include warnings identifying the drawbacks of criminal background checks and recommending precautions daters should perform before meeting in person.[163] Furthermore, by notifying

---

157 *See infra* Part III.C.2 (calculating the economic feasibility of requiring dating websites to perform criminal background checks on users).

158 *See supra* note 27 and accompanying text (recognizing that dating websites recommend dating safety tips and techniques to increase a user's safety but fail to take an active role in improving online dating safety outside of these advisory tips). *But see supra* note 25 (identifying the only dating website to implement criminal background checks into its safety procedures).

159 *See supra* notes 102–03 and accompanying text (examining the depth of current online criminal background checks).

160 Coleman, *supra* note 34, at 183 n.368 (discussing the limitations of requiring dating websites to perform criminal background checks on users).

161 *See supra* note 29 and accompanying text (providing examples of attacks stemming from online dating that background checks may prevent).

162 *See supra* note 40 (reviewing the claim that criminal background checks will grow the problem rather than act as a solution because users will develop a false sense of security).

163 *See supra* note 27 (explaining the safety tips that dating websites provide to users). Currently, dating websites post safety tips within their terms of conditions or on separate pages that users may not view while utilizing the site. *Id.* However, by placing the dating

users of the drawbacks of background checks and providing safety tips along with the background check results, users will remain aware of the dangers involved with online dating and thus will not develop a false sense of security.[164] Beyond the policy decision of whether criminal background checks will reduce or increase the safety of online dating, requiring criminal background checks poses another problem: whether dating websites may remain profitable while implementing checks into their safety procedures.[165]

2. Dating Websites May Withstand the Increased Cost of Criminal Background Checks

Requiring dating websites to perform criminal background checks will pose economic challenges for the websites.[166] However, increasing the volume of background checks performed will reduce the cost of online criminal background checks and make the requirement that dating websites perform background checks economically feasible.[167] For example, Intelius provides a national criminal records check for $39.95, but Intelius also advertises a volume discount, which dating websites may utilize by performing checks for each user.[168] If a dating website requires each user to pay for the annual criminal records check, the dating website must increase each user's monthly fee by $3.33 to break even.[169] Although a $3.33 increase may dramatically reduce the

---

tips within the notification for criminal background check results, the dating safety tips will be more accessible and users will view the tips more often, which in turn will reduce the alleged false sense of security. *See supra* note 40 (providing an overview of the false sense of security that may result from criminal background checks).

164 *See supra* note 40 (providing an overview of the false sense of security resulting from criminal background checks); *see also* Horcher, *supra* note 108, at 273–74 (questioning whether a false sense of security is worse than no security at all). Additionally, users develop a false sense of security by using the website successfully even if the website does not perform criminal background checks on users. *Id*.

165 *See infra* Part III.C.2 (assessing the economic challenges of requiring dating websites to perform criminal background checks on users).

166 *See supra* note 105 (indicating the cost of providing criminal background checks for users).

167 *See supra* note 105 (identifying popular online criminal background check providers, and the current costs of performing one national check from each provider).

168 *See supra* notes 100, 105 (stating the price of Intelius's national criminal records check along with the information the check will provide); *see also supra* note 106 and accompanying text (providing the volume pricing for an Intelius background check).

169 *See supra* notes 105–06 (examining Intelius's costs and volume discount offering). The price increase calculation relates to using Intelius as the provider and fails to include a likely volume discount. *See supra* notes 105–06. However, dating websites may choose cheaper alternatives instead of Intelius, opting for criminal background checks as low as $12.95. *See supra* note 105 (listing the price of criminal background checks by Sentry Link

number of users of free online dating providers, the most popular dating websites charge $30 to $60 a month; therefore, a $3.33 increase in monthly fees seems reasonable.[170] Furthermore, True.com requires its users to submit to a criminal background check and currently charges $50 a month, thus demonstrating the feasibility of performing criminal background checks on all users.[171]

In sum, dating websites may perform criminal background checks while remaining economically viable, and these background checks will decrease the dangers of online dating.[172] However, states do not currently require dating websites to perform criminal background checks.[173] Therefore, Part IV proposes a model state statute mandating that dating websites perform criminal background checks on all users.[174]

IV. CONTRIBUTION

Although online dating is inherently risky—meeting someone in person for the first time—an online dating website should not receive immunity after placing someone in a dangerous situation by recommending a date with a convicted criminal.[175] Under current law, online dating websites may avoid a negligence claim, for failure to perform criminal background checks, by claiming immunity under the CDA or arguing no duty exists to perform criminal background checks.[176] Many proposals seek to amend the CDA by removing a

---

or U.S. Criminal Checks). By choosing a cheaper alternative with a volume discount, dating websites may limit the monthly increase to $1.00.

170 *See supra* note 21 and accompanying text (comparing the monthly fees of popular online dating services).

171 *See supra* note 25 (discussing that True.com utilizes criminal background checks to screen users but remains competitive with other dating services by only charging $50 a month); *see also* Horcher, *supra* note 108, at 271–72 (disclaiming that fee-charging dating websites cannot remain profitable when implementing background checks on users).

172 *See supra* Part III.C (analyzing that criminal background checks will increase dating safety and not place a significant economic burden on dating websites).

173 *See supra* Parts II.B, III.B (recognizing that states do not require dating websites to perform criminal background checks on users and instead courts grant websites immunity under the CDA).

174 *See infra* Part IV.A (proposing a state statute that requires dating websites to perform criminal background checks and notify users of each recommended date's criminal history).

175 *See supra* note 28 (discussing situations where online dating websites recommended users with criminal convictions to other users).

176 *See supra* Part III.B (analyzing why the CDA grants immunity to online websites from negligence claims and recognizing that an online dating website does not have a duty to perform criminal background checks on users).

website's immunity from negligence claims.[177] However, an amendment to the CDA only solves part of the problem because it only removes the immunity but fails to impose a legal duty to act.[178] Therefore, Part IV proposes a model state statute that imposes a legal duty on online dating websites to perform criminal background checks on users, which will work together with a CDA amendment and allow a victim's negligence claim to reach a jury.[179] Part IV.A proposes a statute requiring dating websites to perform criminal background checks on users and notify users about a recommended date's criminal history.[180] Part IV.B explains the effects of implementing the proposed statute on victims and dating websites.[181]

A. Proposed Model State Statute

Specifically, a model state statute that requires online dating websites to perform criminal background checks could read as follows:

> *Definitions as used in this act:*[182]
> *(a) "'Internet dating service' means a person or entity directly or indirectly in the business, for profit, of offering, promoting or providing access to dating, relationship, compatibility, matrimonial or social referral services principally on or through the Internet."*[183]
> *(b) "'Member' means a customer, client or participant who submits to an Internet dating service information required to access the service for the purpose of engaging in dating, relationship, compatibility, matrimonial or social referral."*[184]

---

177 *See supra* note 98 (listing different proposed amendments to the CDA to remove website immunity from tort claims).

178 *See supra* Part II.D.1 (demonstrating that a victim must prove a dating website's duty to perform criminal background checks to succeed in a negligence claim against the website).

179 *See infra* Part IV (suggesting that states enact a model statute that imposes a legal duty on online dating websites to perform criminal background checks on users).

180 *See infra* Part IV.A (proposing a model state statute that imposes a duty on dating websites to perform criminal background checks and notify users of each recommended date's criminal record).

181 *See infra* Part IV.B (highlighting the benefits of enacting the proposed state statute).

182 The definitions in this act are modeled or taken from N.J. STAT. ANN. § 56:8-170 (West, WestlawNext through L.2013, c. 84 and J.R. No. 9) (defining terms used in the New Jersey statute that requires online dating websites to notify users if the website performs criminal background checks).

183 *Id.* § 56:8-170d.

184 *Id.* § 56:8-170f.

(c) "'Criminal background screening' means a name search for a person's criminal convictions initiated by an on-line dating service provider and conducted by one of the following means:

(1) By searching available and regularly updated government public record databases for criminal convictions so long as such databases, in the aggregate, provide substantial national coverage; or

(2) By searching a database maintained by a private vendor that is regularly updated and is maintained in the United States with substantial national coverage of criminal history records and sexual offender registries."[185]

(d) "'Criminal conviction' means a conviction for any crime including but not limited to any sex offense that would qualify the offender for registration pursuant to [insert applicable state statute] or under another jurisdiction's equivalent statute."[186]

(e) "Violent offenses" means a conviction including but not limited to battery, assault, burglary, or robbery.

(f) "Sex offenses" means a conviction including but not limited to rape, sexual assault, sexual harassment, or stalking.

(g) "Fraudulent offenses" means a conviction including but not limited to identity theft, embezzlement, or credit card fraud.

(h) "Recommended match" means a member chosen as a potential date for another member by the Internet dating service based on each member's dating profile.[187]

An Internet dating service shall:

(a) perform annual criminal background screenings on all members;

(b) notify members of the criminal background screening results for each recommended match;

(1) the notification of the criminal background screening results shall include:

A. the number of convictions;

B. the type of each conviction; and

---

185 *Id.* § 56:8-170a.

186 *Id.* § 56:8-170h.

187 The definitions for violent offenses, sex offenses, fraudulent offenses, and recommended match are the contribution of the author.

C. the date of each conviction for:
i. all felony convictions; and
ii. misdemeanor convictions involving
1. violent offenses;
2. sex offenses; and
3. fraudulent offenses
(2) the Internet dating service shall provide a member with the results at the same time the website recommends the match
(c) allow members to choose not to receive any recommended matches with a prior criminal conviction.[188]

B. Commentary

The proposed statute affects both victims and dating websites and serves two policy interests.[189] Part IV.B.1 demonstrates how the proposed statute improves user safety when using dating websites.[190] Part IV.B.2 explains how the proposed statute imposes a duty on dating websites and grants victims an opportunity to hold dating websites accountable for failing to perform criminal background checks.[191]

1. Increasing User Safety on Dating Websites

Requiring that dating websites perform criminal background checks and notify each user of a recommended date's criminal history will increase user safety.[192] With the proposed statute, dating websites will identify dangerous individuals who use the online dating service and users will become aware of their recommended dates' criminal history.[193] As a result, dating websites may refuse to provide their services to dangerous individuals, or users may decide not to date dangerous individuals. Opponents of mandatory criminal background checks mistakenly claim the checks will create a false sense of security among

188 The duties imposed on an internet dating service are the contribution of the author.
189 *See infra* Parts IV.B.1–2 (explaining that state statutes should increase safety for users of online dating websites and establish a duty that allows victims to hold the websites accountable).
190 *See infra* Part IV.B.1 (discussing how the proposed statute will further protect users).
191 *See infra* Part IV.B.2 (examining how the proposed statute allows victims to hold dating websites accountable rather than allowing websites to escape liability).
192 *See supra* Part II.A (discussing the dangers of online dating including attacks on users by their recommended dates).
193 *See supra* notes 28–29 (explaining that online dating involves an unknown risk of whether a dater previously committed a violent or sexual offense).

users.[194] However, dating websites may attach warnings stating criminal checks fail to catch all dangerous individuals along with recommended safety tips to prevent users from attaining a false sense of security.[195] Furthermore, the current safety procedures, recommending that users follow safety tips for online dating and notifying users whether the site performs criminal background checks, have failed to prevent dangerous individuals with prior convictions from attacking their dates.[196]

In addition, opponents contend that requiring users to submit to a background check presents privacy issues.[197] In order to submit to a criminal background check, users must provide additional information not required to join a dating website.[198] Criminal background checks may require a person's name, birthdate, social security number, and prior addresses for the previous seven years; whereas, dating websites require a person's name, birthdate, address and sometimes credit card information if the website charges fees.[199] By requiring background checks, these websites force users to provide a social security number and a lengthier home address history which arguably invades an individual's privacy.[200] However, the benefit of reducing, or even eliminating, attacks by dangerous users outweighs the cost of requiring users to provide additional personal information.[201] Additionally, by only notifying users of a criminal conviction when the site recommends a potential date, users retain more privacy than if the dating website posted the users' criminal conviction on the users' profile page.[202] In

---

194 *See supra* note 40 (describing that opponents believe providing background checks will create a false sense of security among users).

195 *See supra* Part III.C.1 (arguing that dating websites may prevent a false sense of security among users by providing criminal background checks and safety notifications).

196 *See supra* Part III.A (assessing the failure of current safety procedures to prevent attacks stemming from online dating).

197 *See supra* note 109 and accompanying text (arguing that industry officials believe submitting to background checks will create privacy issues).

198 *Compare* Part II.A (identifying the information users must provide to join a dating website), *with* Part II.E (discussing the information required to perform a criminal background check).

199 *Compare* Part II.E (explaining the required information for a criminal background check), *with* Part II.A (providing an overview of the information required on online dating websites).

200 *See supra* note 109 and accompanying text (recognizing the industry's argument that background checks infringe on a user's privacy).

201 *See supra* Part III.C.1 (highlighting the safety benefits of requiring dating websites to perform criminal background checks).

202 *See* Horcher, *supra* note 108, at 276 (proposing a federal statute that requires dating websites to place a notification on the user's profile page indicating a prior felony or sex offense conviction). This Note's proposed statute grants users more privacy because the statute only requires dating websites to notify users of prior convictions when the website

addition to increasing user safety, the proposed statute grants victims an opportunity to hold a website accountable for its actions.[203]

2. Allowing Users to Hold Dating Websites Accountable

The proposed statute imposes on dating websites a legal duty to perform criminal background checks and notify users of their recommended date's criminal history.[204] The statute allows a victim to establish a dating website's duty to perform criminal background checks and a website breaches that duty if it fails to perform criminal background checks.[205] Thus, a victim capable of proving the cause in fact, proximate cause, and damages elements of a negligence claim stemming from a dating website's failure to perform a criminal background check may bring their case to a jury, rather than face a court dismissal because the website has no duty to perform criminal background checks.[206] Yet, to ultimately succeed against a dating website, Congress must enact an amendment to the CDA limiting immunity from negligence actions.[207]

An amendment to the CDA should reduce the amount of immunity granted to websites from tort claims. An amendment may propose a balancing test to weigh the harm caused and the extent to which the website caused the injury or may simply reduce immunity to claims involving copyright and defamation causes of action.[208] This two-part solution will allow a victim attacked by her recommended online date to bring her claim to a jury, rather than having the claim summarily dismissed.

---

recommends a potential match, rather than allowing all users to view the criminal conviction on the user's profile page.

203 *See infra* Part IV.B.2 (discussing that the proposed statute presents victims with an opportunity to hold dating websites accountable for failing to perform criminal background checks).

204 *See supra* text acccompanying note 188 (imposing on an internet dating service various duties that would notify a victim of a potential date's criminal history); *see also* Part II.D.1 (defining the legal duty required to prove a negligence claim).

205 *See supra* notes 73–77 and accompanying text (discussing the duty of care standard and breach thereof in a negligence cause of action).

206 *See supra* Part II.D (explaining the required elements in a negligence action and recognizing that a victim may prove multiple elements of the claim for a dating website's failure to perform criminal background checks, but that a duty failed to exist under current legislation).

207 *See supra* Part II.D.2 (examining CDA decisions granting broad immunity to websites from tort claims).

208 *See supra* note 98 (listing—among other possible CDA amendments—a balancing test considering all the circumstances and a solution that would use the CDA only for copyright and defamation claims rather than tort claims).

V. CONCLUSION

The increase in social networking and online dating connects people that would never meet, but it also provides criminals with more access to possible victims.[209] Currently, most online dating websites fail to perform criminal background checks on users, thus failing to protect users from someone with a criminal background.[210] This allows online dating websites to recommend, as a potential match, a user with an extensive criminal background. Unfortunately, when a user with a criminal background attacks his recommended date, the victim cannot recover from the online dating website for its failure to perform criminal background checks on its users.[211]

An online dating website may escape liability by claiming immunity under the CDA or claiming no duty exists to perform criminal background checks.[212] Therefore, although a victim may prove that the online dating website's failure to perform a criminal background check was the cause in fact and proximate cause of the victim's damages, a court will likely grant summary judgment against the victim when considering a claim of negligence. Many commentators have proposed amendments to the CDA to remove immunity from tort claims for websites.[213] Yet, an amendment to the CDA will not allow a victim to surpass summary judgment against an online dating website. Therefore, this Note proposed a model state statute that requires online dating websites perform criminal background checks on users and notify users of their recommended dates' results. In addition, the proposed statute established a legal duty for online dating websites to perform criminal background checks, which will allow a victim to surpass summary judgment and bring her claim before a jury.[214]

Returning to the story of Sam, a young woman attacked by her recommended date—with a criminal background—while using an online dating website; imagine if the online dating website had performed a criminal background check on Sam's date and notified her of his prior convictions, rather than allowing Sam to believe she found the perfect match. Under this scenario, the online dating website would warn Sam

---

209 *See supra* notes 28–29 (discussing criminal attacks resulting from online dating).

210 *See supra* note 25 (recognizing that currently only True.com performs criminal background checks on users).

211 *See supra* Part II.C (discussing the case law that grants websites immunity under the CDA).

212 *See supra* notes 85, 91 (noting cases granting immunity to websites from tort claims).

213 *See supra* note 98 (listing proposed solutions to change CDA immunity).

214 *See supra* Part IV.A (proposing a model state statute requiring dating websites to perform criminal background checks).

of her recommended date's criminal history, and Sam would likely decide not to date that user, which would have prevented her eventual rape and sexual assault.

Ryan D. O'Day[*]

[*] J.D. Candidate, Valparaiso University Law School (2014); B.S., Management, Purdue University (2011). I would like to thank my wife, Kelly, for her constant love, support, and sacrifice throughout my law school career. Thank you to my parents, Steve and Debbie, for their love, support, and guidance, which made me the person I am today. Thank you to my siblings, Rory, Raeanne, and Rilee, for pushing me to set a good example and reminding me to continue to have fun. Lastly, I would like to thank the Volume 47 Executive Board for their time, comments, and assistance throughout the note writing process.