APPLYING THE COMMON-LAW CAUSE OF ACTION NEGLIGENT ENABLEMENT OF IMPOSTER FRAUD TO SOCIAL NETWORKING SITES

Shannon N. Sterritt [*]

> But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed.[1]

I. INTRODUCTION

Social networking sites, such as MySpace, Twitter, Facebook, and LinkedIn, are popping up all over the Internet and establishing social media as the fastest-growing phenomenon yet. While radio took thirty-eight years to reach fifty million users and television took thirteen years, the Internet took only four years.[2] Social networking sites, however, quickly surpassed these records. Facebook reached over fifty million users within thirteen months of allowing access to anyone with a valid email address.[3] Today, while continuing to grow at a rapid pace, Facebook has more than 750 million users.[4] LinkedIn, a professional social networking site, reached thirty-six million members in March 2009 and is adding members at a rate of one member per second.[5]

---

[*] J.D., 2011, Seton Hall University School of Law; B.A., 2008, University of Maryland—College Park. I would like to thank Professor Ronald J. Riccio and Seth Fersko for all of their help and guidance throughout this process and my parents for their continuous love and support.

[1] WILLIAM SHAKESPEARE, OTHELLO act 3, sc. 3.

[2] United Nations, *Information and Communications Technology*, UN CYBERSCHOOLBUS 1, http://www.un.org/cyberschoolbus/briefing/technology/tech.pdf (last visited Aug. 14, 2011).

[3] *Timeline*, FACEBOOK, http://www.facebook.com/home.php?ref=home#!/press/info.php?timeline (last visited Aug.14, 2011).

[4] *Statistics*, FACEBOOK, http://www.facebook.com/facebook?ref=pf#/press/info.php?statistics (last visited Aug. 14 2011).

[5] Abbey Klaassen, *LinkedIn Skyrockets as Job Losses Mount*, ADVER. AGE (Mar. 2, 2009), http://adage.com/digital/article?article_id=134962; *see also About Us*, LINKEDIN, http://press.linkedin.com/about (last visited Aug. 14, 2011) ("As of June 30, 2011 (the end of the second quarter), professionals are signing up to join LinkedIn at a rate that is faster than two new members per second. . . . As of August 4,

Social networking sites provide benefits for users of all ages and backgrounds. Social networking sites allow users the ability to reconnect with old friends and make new friends.[6] These websites offer users an open forum for public debate on just about any topic imaginable,[7] which encourages freedom of speech and expression. In addiaddition, most social networking sites are "global," which provides for diverse relationships.[8] Social networking sites are highly effective in the world of advertising and sales.[9] These websites offer traditional Internet advertising options in addition to "fan pages" and "groups," which provide an interactive way to target consumers.[10] Websites created for professional networking and employment searching, such as LinkedIn, also exist within the social networking realm.[11] Studies show that social networking sites also provide educational and developmental benefits to younger users.[12]

While the growth of these websites is indicative of their many benefits, these websites are becoming a dangerous tool. In recent years, stories of crimes facilitated by the use of social networking sites dominated the news. Stories range from Lori Drew, who used MySpace to "cyberbully" her daughter's thirteen year-old rival,[13] to the

2011, LinkedIn operates the world's largest professional network on the Internet with more than 120 million members in over 200 countries and territories.").

[6] *See* Karen Goldberg Goff, *Social Networking Benefits Validated*, WASH. TIMES (Jan. 28, 2009, 5:45 AM), http://www.washingtontimes.com/news/2009/jan/28/social-networking-benefits-validated/.

[7] *See* WHAT IS SOC. NETWORKING, http://www.whatissocialnetworking.com/ (last visited Aug. 14, 2011).

[8] *See id.*

[9] *See* Jean Halliday, *Honda's 'Social Experiment' Nets More than 100,000 Facebook Fans*, ADVER. AGE (Oct. 22, 2009), http://adage.com/article?article_id=139855 (discussing Honda's success in recruiting fans to the brand's Facebook page entitled "Everybody Knows Somebody Who Loves a Honda").

[10] *Id.*

[11] *See About Us*, LINKEDIN, http://press.linkedin.com/about/ (last visited Aug. 14, 2011).

[12] *See, e.g.*, Mizuko Ito et al., *The MacArthur Foundation Reports on Digital Media and Learning; Living and Learning with New Media: Summary of Findings from the Digital Youth Project*, MACARTHUR FOUND., (Nov. 2008), http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-TwoPageSummary.pdf; *Educational Benefits of Social Networking Sites Uncovered*, SCI. DAILY (June 21, 2008), http://www.sciencedaily.com/releases/2008/06/080620133907.htm.

[13] Jennifer LeClaire, *MySpace Mom Indicted in Cyber-Bully Suicide Case*, SCI-TECH TODAY (May 18, 2009), http://www.sci-tech-today.com/news/MySpace-Mom-Charged-in-Teen-Death/story.xhtml?story_id=10300CL7QBNV (discussing the indictment of Lori Drew who created a fake MySpace profile to bully her daughter's rival, who committed suicide as a result).

Craigslist murders[14] and sexual assaults.[15] In addition to these crimes, instances of identity theft have escalated as social networking sites have become more popular.[16] A recent Gallup Crime Survey indicated that identity theft provokes greater concern among Americans than any other crime, with two in three adults worried about falling victim to identity theft.[17]

Identity theft through the use of social networking sites can occur in two different ways: (1) an imposter can gather an individual's personal information, such as name, address, and phone number, from an existing social networking profile and then use it to obtain credit or gain employment in the victim's name, as well as gain access to already established accounts, or (2) an imposter can use another's information to create a false profile on a social networking site, which can then result in harm to one's reputation and possibly one's financial and criminal record. In addition, this latter form of identity theft through social networking sites can lead to other crimes facilitated through the Internet.

Although all of the problems associated with social networking sites are important and deserve lengthy discussion on what the law can do to solve or minimize the effects of these problems, this Comment will focus on the second scenario, that is, when an identity thief uses an individual's information to create a fake profile. Although some imposters might create these fake profiles out of jest, the result

---

[14] *Med Student Arrested In Craigslist Murder*, CBS NEWS (Apr. 20, 2009) http://www.cbsnews.com/stories/2009/04/20/national/main4958272.shtml (detailing an arrest made in the murder of a Boston woman who advertised services on Craigslist)

[15] *See, e.g.*, Shannon Powell, *Craigslist Ad Leads to Sexual Assault*, KXAN.COM (June 11, 2009), http://www.kxan.com/dpp/news/crime/Craigslist_ad_leads_to_sexual_assault (discussing the sexual assault of an Austin woman who had arranged to meet the perpetrator through Craigslist).

[16] "Social networking sites like Facebook and Twitter are the new frontier in the identity theft battle because of their astounding growth rates." Tom Ahearn, *Users of Popular Social Networking Sites Facebook and Twitter Warned About Identity Theft*, MY BACKGROUND CHECK BLOG (Oct. 21, 2009, 11:16 AM), http://www.mybackgroundcheck.com/blog/post/2009/10/21/Users-of-Popular-Social-Networking-Sites-Facebook-and-Twitter-Warned-About-Identity-Theft.aspx.

[17] Lydia Saad, *Two in Three Americans Worry About Identity Theft*, GALLUP (Oct. 16, 2009), http://www.gallup.com/poll/123713/Two-in-Three-Americans-Worry-About-Identity-Theft.aspx. The Poll showed that sixty-six percent of adults in the United States worry frequently or occasionally about identity theft. *Id.* The second biggest concern was a car brake-in or a car theft, which worried forty-seven percent of Americans. *Id.*

of such jokes causes serious harm to their victims.[18] Of more concern, however, are those criminal imposters who create fake profiles with the intent to harm their victims.

This form of imposter fraud is a growing issue for celebrities, who have frequently discovered profiles on social networking sites that they did not create. In 2007, Prince William had a fake Facebook profile of "William Wales" removed from the site.[19] Earlier that year, Sarah Palin sent a message through her Twitter account "AK-GovSarahPalin" apologizing for false information coming from an imposter behind the fake Twitter account "EXGovSarahPalin."[20] The manager of the St. Louis Cardinals, Tony LaRussa, had a fake Twitter account taken down when the perpetrator posted "derogatory and demeaning" messages about his DUI charge and the death of two Cardinals players.[21] And more recently, imposters created fake MySpace and Facebook profiles in the names of Penguins' players Sidney Crosby and Evgeni Malkin to solicit money from the public for the stated, but false, purpose of benefiting a Minneapolis park.[22]

The imposter problem, however, extends beyond the world of the famous and affects the average person, who most likely does not have the resources or clout to fix the problem before serious harm results. In Oregon, Cynthia Barnes's ex-boyfriend created a fake Yahoo profile in her name, which included her address, phone number, and nude photographs of her.[23] In San Antonio, Texas, high school students created a fake MySpace profile of the assistant principal containing false information about her sexual orientation and practices, as well as obscene comments and content.[24] The numerous examples of imposter profiles surfacing on social networking sites show the prevalence of the problem and the potential harm.[25]

---

[18] David Wood, *No Easy Remedy for Imposter Postings on Social Networking Sites*, CONSUMER AFF. (Mar. 17, 2008), http://www.consumeraffairs.com/news04/2008/03/myspace_impostors.html.

[19] Jason Cato, *Great Fake Out: Cyber-Posers Make Life Tough for Celebs*, PITTSBURGH TRIB. REV. (July 16, 2009) (on file with author).

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] Wendy Davis, *Texas Lawmakers Crackdown on Fake Profiles*, MEDIA POST NEWS (June 8, 2009), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=107518.

[24] Chris Gatewood, *Fake User Profiles: Free Speech or Defamation*, SITEPOINT (Nov. 7, 2008), http://articles.sitepoint.com/article/fake-social-networking-profiles.

[25] *See* Wood, *supra* note 18 (describing cases of imposter fraud on social networking sites).

The common-law tort of negligent enablement of imposter fraud, however, may be the solution to this growing problem. Negligent enablement of imposter fraud has traditionally (but sparingly) been used in the context of financial institutions;[26] however, this cause of action is still viable in the social networking site context. This Comment argues that a third party can hold social networking sites liable for their failure to prevent imposter fraud from occurring through the cause of action of negligent enablement of imposter fraud. Although the Communications Decency Act's (CDA or "the Act") immunity provision has been a traditional bar to most lawsuits against social networking sites, recent reinterpretations suggest a narrower reading of the immunity statute, which would allow for claims in the instance of imposter fraud.[27] In the alternative, Congress should amend the Act, explicitly allowing for the prevention of imposter fraud.

This Comment argues that social networking sites are at risk for liability under negligent enablement of imposter fraud because they owe a duty to the public-at-large to attempt to prevent imposter fraud. A social networking site's failure to impose reasonable procedures is therefore a breach of that duty. Expanding the tort of negligent enablement of imposter fraud into the realm of social networking sites will give victims of imposter fraud a remedy and force these sites to put reasonable verification standards in place, ultimately decreasing the prevalence of identity theft on these sites.

Part II of this Comment explores how social networking sites function and how the law has defined identity theft. Part II further details the existing legislation governing social networking sites. In addition, Part II also looks at the current legislation addressing identity theft and the ineffectiveness in providing relief to victims of imposter fraud on social networking sites. Part III proposes expanding the common-law tort of negligent enablement of imposter fraud as a solution to this problem. Part III shows how the CDA is no longer a bar to such a cause of action, and how plaintiffs could succeed on their claims.

II. BACKGROUND

Social networking sites dominate the current age with a majority of individuals having at least one social networking account. With this craze, however, came an increase in identity theft of all forms.

[26] *See infra* Part III.A.

[27] *See infra* Part II.C.

Although there are federal and state statues criminalizing identity theft and attempting to curb its prevalence, unfortunately, imposter fraud on social networking sites presents a whole set of problems that are not regulated by the current statutes.

A. Social Networking Sites: New Age Means of Communication

Social networking sites, such as MySpace, Facebook, and Twitter, dominate the Internet and have forever changed the way people interact and communicate. The features offered on social networking sites vary from site to site; however, most sites center on the idea of a user-maintained profile that is linked to other users of the site through communities and networks.[28] As the court in *Doe v. MySpace, Inc.* explained,

> [S]ocial networking web site[s] . . . allow[] [their] members to create online "'profiles,"' which are individual web pages on which members post photographs, videos, and information about their lives and interests. The idea of online social networking is that members will use their online profiles to become part of an online community of people with common interests. Once a member has created a profile, she can extend "'friend invitations" 'to other members and communicate with her friends . . . via e-mail, instant messaging, or blogs.[29]

Social networking sites are a fun, interactive form of communication and provide entertainment for users of all ages and interests.[30] In addition, social networking sites provide networking benefits, both personal and professional. The use of "groups," "fan pages," and other similar features provide mechanisms to locate users with common interests. In addition, some social networking sites provide a fo-

[28] Richard M. Guo, Note, *Stranger Danger and the Online Social Network*, 23 BERKELEY TECH. L.J. 617, 619–20 (2008). Communities and networks are akin to "small rural communities or neighborhood subdivisions." WHAT IS SOC. NETWORKING, http://www.whatissocialnetworking.com/ (last visited Aug. 14, 2011).

[29] 474 F. Supp. 2d 843, 845–46 (W.D. Tex. 2007).

[30] Facebook's user population is made up of forty-two percent ages eighteen to thirty-four, twenty-two percent ages thirteen to seventeen, twenty percent ages thirty-five to forty-nine, twelve percent ages fifty and over, and four percent ages three to twelve. QUANTCAST, http://www.quantcast.com/ (then type Facebook or MySpace to generate current demographic results) (last visited Aug. 14, 2011). MySpace generates roughly the same demographic proportions. *Id.* Women aged fifty-five or older are the fastest growing group of users on Facebook. Justin Smith, *Fastest Growing Demographic on Facebook: Women Over 55*, INSIDE FACEBOOK (Feb. 2, 2009), http://www.insidefacebook.com/2009/02/02/fastest-growing-demographic-on-facebook-women-over-55/.

rum specifically for professional networking.[31] A recent survey regarding job recruitment indicated that eighty percent of employers use or plan to use social networking sites to find employees.[32]

The most popular social networking sites are Facebook, MySpace Twitter, and LinkedIn.[33] "Unique visitors" refers to the number of individual people who have visited a particular site one or more times within a designated time period.[34] As of October 1, 2011, Facebook has approximately 700,000,000 unique visitors per month, while MySpace has 80,500,000 unique visitors.[35] Twitter and LinkedIn, more recent sites, have quickly jumped in the rankings with 200,000,000 and 100,000,000 unique visitors per month, respectively.[36] Although many social networking sites exist, this Comment will focus on MySpace and Facebook, two of the oldest and most popular social networking sites.

1. MySpace

MySpace began the social networking craze in 2003.[37] Over the years, MySpace made improvements and additions to the site, but the basic format has remained the same. Individuals join MySpace by entering a name, date of birth, gender, and valid email address.[38] After registering, members enter their personal information on topics ranging from "About Me" and "Who I'd Like to Meet," to more specific topics, such as an individual's schools, companies, marital status,

[31] *See, e.g.*, *About Us*, LINKEDIN, http://press.linkedin.com/about (last visited Aug. 14, 2011).

[32] *Jobvite Survey Reveals Untapped Potential in Social Networks*, JOBVITE (May 13, 2008), http://recruiting.jobvite.com/news/press-releases/pr/social-recruitment-survey-release.php. The survey indicates that employers are recruiting more heavily through social networking sites. *Id.*

[33] *Top 15 Most Popular Social Networking Sites, October 2011*, EBIZMBA (Oct. 1 2011), http://www.ebizmba.com/articles/social-networking-websites [hereinafter *Top Networking Sites*].

[34] Jason Bubury et al., *Web Analytics Definitions—Version 4.0*, WEB ANALYTICS ASS'N, 9 (Aug. 16, 2007), http://www.webanalyticsassociation.org/resource/resmgr/PDF_standards/WebAnalyticsDefinitionsVol1.pdf.

[35] *Top Networking Sites*, *supra* note 33.

[36] *Id.*

[37] *A History of MySpace*, RANDOMHISTORY.COM (Aug. 14, 2008), http://www.randomhistory.com/2008/08/14_myspace.html (discussing MySpace as similar to the already existing social networking site, Friendster); *see also* Guo *supra* note 28, at 621.

[38] *Sign up for MySpace*, MYSPACE, http://signups.myspace.com/index.cfm?fuseaction=signup (last visited Mar. 15, 2011).

hometown, and personal preferences.[39] MySpace members interact by sending messages and "friending" each other.[40] Members can update their profiles to reflect what they are doing and their current mood, as well as post favorite videos, photos, and music playlists.[41] MySpace has a strong focus on the entertainment world and is a popular spot for musicians to showcase their music.[42] In addition, News Corp., MySpace's previous parent company, "helped create MySpace Music," a joint venture with four recording agencies.[43]

With attempts to create a safe networking space, MySpace established terms and conditions, applicable to all users, prohibiting illegal conduct. MySpace's Terms and Conditions provide for the following:

> By using the MySpace Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 13 years of age or older; and (d) your use of the MySpace Services does not violate any Applicable Law.[44]

The Terms and Conditions also prohibit criminal and tortious activity, such as "child pornography, fraud, trafficking in obscene material, drug dealing, gambling, harassment, defamation, stalking, spamming, spimming, sending of viruses or other harmful files, copyright infringement, patent infringement, or theft of trade secrets."[45] Despite these terms, detecting user violations is difficult.

The age of MySpace members varies, ranging from fourteen years old to sixty-five and over; however, trends show MySpace is more popular among younger users.[46] In 2006, MySpace expanded

---

[39] *Profile Edit*, MYSPACE, http://home.myspace.com (username and password required) (last visited Feb. 13, 2011).

[40] *Id.*

[41] *Id.*

[42] Greg Sandoval, *MySpace to Push Deeper into Entertainment*, CNET NEWS (July 10, 2009), http://news.cnet.com/8301-1023_3-10284593-93.html.

[43] *Id.* MySpace was sold in June of 2011 to Specific Media and Justin Timberlake. Andy Fixmer, *News Corp. Calls Quits on MySpace With Specific Media Sale*, BUSINESSWEEK (June 29, 2011 9:59 PM), http://www.businessweek.com/news/2011-06-29/news-corp-calls-quits-on-myspace-with-specific-media-sale.html.

[44] *Myspace.com Terms of Use Agreement*, MYSPACE (June 25, 2009), http://www.myspace.com/help/terms.

[45] *Id.*

[46] Matt Dickman, *The Age of Facebook v. MySpace: February/March Edition*, TECHNOMARTKETER (Mar. 10, 2009, 10:38 PM), http://technomarketer.typepad.com/technomarketer/2009/03/the-age-of-facebook-vs-myspace-februarymarch-edition.html; Manoj Jasra, *Age Differences Between MySpace and Facebook Users*, WEBPRONEWS (Feb. 10, 2010, 3:25PM), http://www.webpronews.com/age-differences-between-myspace-and-facebook-users-2010-02.

its operations by permitting membership internationally and made its website available in several languages.[47] Although it no longer maintains the number one spot, MySpace remains one of the most popular websites in the nation.[48]

2. Facebook

Shortly following MySpace, Facebook launched its site in 2004 from a Harvard dorm room.[49] Although originally restricted to users with a valid university or college ".edu" email address, the site eventually allowed access to users with any valid email address.[50] Similar to MySpace, joining Facebook requires that an individual provide an email address, name, gender, and date of birth.[51] Thereafter, the user is prompted to enter optional information, such as high school name and graduation year, as well as post a profile picture.[52] After joining, members can connect with other members through "friending," posting pictures, updating statuses, creating or joining groups and events, and sending messages to other users. Like MySpace, Facebook also attempts to stop illegal activity from occurring on its site by posting conditions of use that are applicable to all users. Facebook's Statement of Rights and Responsibilities states:

> Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account: You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission . . . .[53]

As of July 2011, Facebook has grown to over 750 million users worldwide.[54] Facebook members, like those of MySpace, vary in age, but the most common members are between the ages of eighteen

---

[47] *See International–MySpace.com*, MYSPACE, http://www.myspace.com/international (last visited Aug. 14, 2011).

[48] *See supra* notes 33–36 and accompanying text.

[49] *#158 Mark Zuckerberg: The Forbes 400 Richest Americans 2009*, FORBES.COM (Sept. 30, 2009), http://www.forbes.com/lists/2009/54/rich-list-09_Mark-Zuckerberg_I9UB.html.

[50] *Timeline*, FACEBOOK, http://www.facebook.com/press/info.php?timeline (last visited Aug. 14, 2011).

[51] FACEBOOK, http://www.facebook.com/ (last visited Aug. 14, 2011).

[52] *Id.*

[53] *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php?ref=p (last visited Aug. 14, 2011).

[54] *Statistics*, FACEBOOK, http://www.facebook.com/facebook?ref=pf#/press/info.php?statistics (last visited Aug. 14 2011).

and twenty-one.[55] On June 15, 2009, Facebook surpassed MySpace in the number of members, both in the United States and worldwide, at a rapid-fire pace.[56]

B. Identity Theft: A Growing Problem

Although identity theft is a well-established crime, it is currently the "fastest-growing crime" in the nation."[57] The Federal Trade Commission estimates that as many as nine million individuals fall victim to identity theft each year.[58] According to federal law, identity theft is the knowing transfer, possession, or use of another's means of identification without authority.[59] One's "means of identification" is defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[60]

Identity thieves target people of all demographics, races, genders, and nationalities. Identity thieves get an individual's private information in a variety of ways—from "basic street theft to sophisticated, organized crime schemes."[61] The most common methods that identity thieves use to obtain another's information are: "dumpster diving," when thieves look through trash for papers with personal information listed; "skimming," when thieves use a special storage device to steal credit-card numbers when individuals make a purchase; and "phishing," when thieves send pop-ups or spam to lure people to give personal information.[62] Once an identity thief has a victim's information in his or her hands, the thief can transact business as the

---

[55] Dickman, *supra* note 46.

[56] Erick Schonfeld, *Facebook Finally Catches up to MySpace in the U.S.*, TECHCRUNCH (June 15, 2009), http://www.techcrunch.com/2009/06/15/facebook-finally-catches-up-to-myspace-in-the-us/.

[57] *Identity Theft*, U. S. POSTAL INSPECTION SERV., https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IdentityTheft.aspx (last visited Aug. 14, 2011); *accord Consumer Resources*, IDENTITY THEFT RECOURSE CENTER, http://www.idtheftcenter.org/c_resources/c_intro.shtml (last visited Aug. 14, 2011).

[58] *About Identity Theft*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Aug. 14, 2011).

[59] 18 U.S.C. § 1028 (2006); *see also* 16 C.F.R § 603.2(a) (2004).

[60] § 1028(d)(7).

[61] S. REP. NO. 105-274, at 6 (1998).

[62] *Take Charge: Fighting Back Against Identity Theft*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm (last visited Aug. 14, 2011). Identity thieves also use a change of address form to divert billing statements to the thieves themselves and listen for personal information shared during a cell phone conversation. *Id.*

victim and sometimes become the victim by living and working under the victim's name.[63] An identity thief can take funds from an individual's bank accounts, incur debts, and even commit crimes in another's name.[64]

Identity thieves use different forms of identity theft to jeopardize an individual's personal or financial information.[65] For example, identity theft occurs when, upon arrest, an identity thief "poses" as another by providing law enforcement with another's personal identifying information.[66] Financial fraud identity theft occurs when an identity thief uses another's identifying information for financial gain, either by opening new accounts in the victim's name or by taking over the victim's already existing accounts.[67] A third form, "identity cloning" or imposter fraud, occurs when an identity thief assumes another's identity by living and working as the victim.[68]

Imposter fraud on social networking sites has recently become popular among identity thieves.[69] This form of imposter fraud occurs when someone uses another's information to create a profile or webpage on a social networking site.[70] Most professionals have enough personal information in the public domain that an identity thief can easily create an accurate and deceiving "online persona" on a social networking site.[71] Once an imposter has created this profile, he or she can act as the victim in the virtual setting by communicating with friends, acquaintances, and colleagues of the victim, which provides a limitless opportunity for damage. An imposter can create difficulties in employment, ruin professional and personal relationships, and damage reputations, as well as steal corporate or financial records and other sensitive information.[72]

---

[63] Om Paramapoonya, *10 Things Identity Theft Victims Must Do*, HUB PAGES, http://hubpages.com/hub/identity-theft-solutions (last visited Aug. 14, 2011).

[64] *Id.*

[65] *Identity Theft (October 2009)*, NAT'L WHITE COLLAR CRIME CTR., http://www.nw3c.org (Follow "Research" then "Papers, Publications, Reports" then "Papers") (on file with author).

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *See* ATTACK INTELLIGENCE RESEARCH CTR., ANNUAL THREAT REPORT: 2008 OVERVIEW AND 2009 PREDICTIONS 13 (2008), *available at* www.hasp.com/pdf/airc/AIRC-Annual-Threat-Report2008.pdf.

[70] *See id.*

[71] *Id.* ("In several experiments performed at the [Attack Intelligence Research Center], as well as other facilities, a simulated fake online persona ended up connecting to the real network of acquaintances rather easily.").

[72] *Id.*

Identity theft in any form takes an incredible toll on its victims. With the potential to ruin a victim's credit and financial history, taint his or her criminal record, and destroy his or her reputation, identity theft is a common fear among Americans.[73] In addition, victims dedicate large amounts of time to clearing their names.[74] Although it has been around for many years, identity theft has increased with the introduction of the Internet. Today, the information needed to steal someone's identity is likely just a few clicks away.

C. Regulation for Social Networking Sites: The Communications Decency Act

Title V of the Telecommunications Act, also known as the CDA,[75] regulates offensive material on the Internet.[76] Section 230 of the CDA states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[77] Courts interpret this statute to provide a broad immunity, which encompasses MySpace and similar social networking websites.[78] The CDA also provides a "Good Samaritan" provision that limits the liability of those providers or users who take action or provide the technical means to restrict access to material that the providers consider obscene.[79]

Congress enacted § 230 in response to *Stratton Oakmont, Inc. v. Prodigy Services Co.*[80] In *Stratton*, the New York Supreme Court for Nas-

---

[73] Saad, *supra* note 17.

[74] *Fighting Identity Theft—The Role of FCRA: Hearing Before the Subcomm. on Fin. Insts. & Consumer Credit of the Comm. on the Judiciary*, 106th Cong. 15 (2002) (statement of Daniel L. Mihalko, Inspector in Charge, Cong. and Pub. Affairs, U.S. Postal Inspection Service) ("It generally takes about 44 months to clear up their cases, and victims report that they spend on average 175 hours actively trying to restore their credit rating and to clear their good name."); *see also* IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH 2008 3 (2009), *available at* http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf (noting that when an imposter opened a new account, victims spent approximately 165 hours clearing their names).

[75] Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C. (1996)).

[76] *See* Ken S. Meyers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 172 (2006).

[77] 47 U.S.C. § 230(c)(1) (2006). "The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server . . . ." § 230(f)(2).

[78] *See* Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 846 (W.D. Tex. 2007).

[79] § 230(c)(2).

[80] No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995); *see* H.R. REP. NO. 104-458, at 194 (1996), *reprinted in* 1996 U.S.C.C.A.N. 10.

sau County held that the interactive computer service provider Prodigy was liable for defamatory statements on its website because its ability to delete offensive material demonstrated its control, which the court found rose to a level similar to that of a publisher over the content of the website.[81] In enacting § 230, Congress disapproved of the *Stratton* decision:

> [Section 230] provides "Good Samaritan" protections from civil liability for providers . . . of an interactive computer service for actions to restrict . . . access to objectionable online material. One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers . . . as publishers or speakers of content that is not their own because they have restricted access to objectionable material.[82]

The § 230 immunity aims "to keep government interference in the medium to a minimum."[83] Representatives Christopher Cox and Ron Wyden, who proposed § 230, wanted to limit the role of the Federal Communications Commission in regulating material on the Internet and instead, using filtering software, place the burden on parents to regulate their children's Internet activity.[84] The CDA lists sevseveral policy goals of the immunity provision:

> 1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
> 2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
> 3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
> 4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
> 5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.[85]

---

[81] *Stratton*, 1995 N.Y. Misc. LEXIS 229, at *13–14.

[82] H.R. REP. NO. 104-458, at 194.

[83] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

[84] *See generally* 141 CONG. REC. H8460–70 (daily ed. Aug. 4, 1995) (Statements of Rep. Cox and Rep. Wyden).

[85] 47 U.S.C. § 230(b) (2006).

The CDA expressly allows states to enact legislation consistent with the CDA; however, states cannot create a cause of action that would be inconsistent with the Act, such as holding an interactive computer service provider or user liable as the publisher of information produced by another information content provider.[86]

Much of the litigation that has involved social networking sites has focused on the CDA-immunity issue. The past disputes that raised the CDA-immunity issue arose in the context of defamation and other negligence claims as well as suits involving online sexual predators. For example, in *Zeran v. America Online, Inc.*, anonymous postings of offensive advertisements, which contained the plaintiff's contact information, caused the plaintiff to receive death threats and other harassing phone calls.[87] The U.S. Court of Appeals for the Fourth Circuit, addressing whether America Online could be held liable for failing to remove advertisements after being notified of their fraudulent nature, held that the CDA, "[b]y its plain language, . . . creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[88] The court also noted that imposing liability in such a situation would force website operators to screen every posting on their websites and thoroughly investigate every complaint of defamation—an impossible burden.[89]

Almost ten years later, in *Doe v. MySpace*, the U.S. District Court for the Western District of Texas extended the immunity to social networking sites.[90] Thirteen-year-old Julie Doe was sexually assaulted by a nineteen-year-old male whom she met through MySpace.[91] The court rejected the plaintiff's argument for a narrow interpretation of § 230 immunity and thus excluded her claim of negligent failure to implement basic safety measures to prevent sexual predators from communicating with minors.[92] The plaintiff argued that her claim fell outside the scope of § 230 because she did not base her claim on third-party content and did not direct her claim at the site in its capacity as an editor or publisher.[93] The court noted several cases in which courts granted § 230 immunity for claims of negligence and

[86] § 230(e)(3).
[87] 129 F.3d 327, 329 (4th Cir. 1997).
[88] *Id.* at 330.
[89] *Id.* at 331, 333.
[90] 474 F. Supp. 2d 843, 846, 849–50 (W.D. Tex. 2007).
[91] *Id.* at 846.
[92] *Id.* at 848–50.
[93] *Id.* at 848.

declined to restrict the immunity to claims involving defamation or actions involving the content of the information on the website.[94]

Recently, however, courts have reconsidered past interpretations of the CDA that gave Internet service providers (ISPs) blanket immunity from all civil-liability claims.[95] For example, although ultimately finding that Craigslist was not liable for information posted by a third party, in *Chicago Lawyers' Committee v. Craigslist*, the U.S. Court of Appeals for the Seventh Circuit reinterpreted § 230 immunity: "Subsection (c)(1) does not mention 'immunity' or any synonym. . . . [Section] 230(c) as a whole cannot be understood as a general prohibition of civil liability for web-site operators and other online content hosts."[96] Quoting an earlier opinion to explain its holding, the court questioned, "Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?"[97]

The U.S. Court of Appeals for the Ninth Circuit agreed that the traditionally broad immunity should be construed more narrowly than courts had in the past. In *Fair Housing Council v. Roommates.com*, the court held that Roommates.com was not entitled to § 230 immunity because it became an information content provider through its standardized questionnaire.[98] The court noted that Congress passed § 230 to allow ISPs the opportunity to engage in some editing of user-generated content without the risk of becoming liable for the defamatory content they did not edit or delete.[99] The CDA "was not meant to create a lawless no-man's-land on the Internet."[100] A more recent Ninth Circuit decision reaffirmed the *Roommates.com* reinterpretations by holding that the immunity provision applies only when a provider or user of an interactive computer service is being treated

[94] *Id.* at 849. The *Doe* court also considered the case under Texas common law and determined that no legal duty existed to hold the social networking site liable under a theory of common-law negligence. The court determined that requiring a duty to confirm or determine the age of applicants would "stop MySpace's business in its tracks," ultimately shutting down this method of communication. *Id.* at 851.

[95] *See, e.g.*, Fair Hous. Council v. Roomates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008); Chi. Lawyers' Comm. for Civil Rights Under Law v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008).

[96] 519 F.3d at 669.

[97] *Id.* at 670 (quoting Doe v. GTE Corp., 347 F.3d 655, 659–60 (7th Cir 2003)).

[98] 521 F.3d at 1164.

[99] *Id.* at 1163.

[100] *Id.* at 1164.

as the publisher or speaker of information provided by another user of the site.[101]

D. Regulations for Identity Theft

Because identity theft is an increasing problem in the United States, state and federal legislatures have continually returned to the drawing board to enact laws to cover all facets of the crime. Over the years, legislatures have enacted statutes that range from laws establishing identity theft as a crime to those regulating privacy and data collection in an attempt to prevent identity theft from occurring in the first place. But as the times and technology keep progressing, various methods of identity theft fall outside the reach and protection of the law and thus provide little remedy or help to victims.

1. Federal Regulations

Although federal laws have made great strides in combating identity theft, the number of victims affected by the crime continues to increase.[102] In 1998, Congress established identity theft as a crime through the Identity Theft and Assumption Deterrence Act.[103] The Act imposes criminal penalties upon offenders, including fines and up to fifteen years of imprisonment.[104] Although the unauthorized use or transfer of identifying *documents* and credit cards was illegal prior to 1998, the Act added a provision criminalizing the use or transfer of identifying *information*.[105] By doing so, Congress recognized that criminals do not need documents to assume another's identity; they generally just need the information.[106] Congress later enacted the Internet False Identification Prevention Act, which covers exclusively problems of identity theft stemming from the Internet.[107] The Act expanded 18 U.S.C. § 1028 to include as a crime the use of the Internet to transfer fraudulent or counterfeit documents.[108]

---

[101] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100–01 (9th Cir. 2009).

[102] *2009 Identity Theft Statistics*, SPENDONLIFE, http://www.spendonlife.com/guide/2009-identity-theft-statistics (last visited Aug. 14, 2011) (stating that between 2007 and 2008 the number of identity-theft victims increased twenty-two percent).

[103] Pub. L. No. 105-318, 112 Stat. 3007 (codified as 18 U.S.C. § 1028 (2006)).

[104] *Id.*; U.S. GENERAL ACCOUNTING OFFICE, GAO-02-766, IDENTITY THEFT: AWARENESS AND USE OF IDENTITY THEFT DATA 1 (2002), *available at* http://www.gao.gov/new.items/d02766.pdf.

[105] U.S. GENERAL ACCOUNTING OFFICE, *supra* note 104, at 1.

[106] 18 U.S.C. § 1028(a)(7); *see* U.S. GENERAL ACCOUNTING OFFICE, *supra* note 104.

[107] Pub. L. No. 106-578, 114 Stat. 3075 (codified at 18 U.S.C. § 1028 (2006)).

[108] *See id.*

Congress also imposed an "affirmative and continuing obligation" on financial institutions to protect consumers' privacy.[109] The Gramm-Leach-Bliley Act requires financial institutions to put appropriate standards in place to protect against threats to the security or integrity of customer records and unauthorized access or use of customer records and information.[110]

In addition, Congress enacted the Federal Credit Reporting Act[111] "to "promote efficiency in the Nation's banking system and to protect consumer privacy."[112] The Act requires that credit-reporting agencies create reasonable procedures to assure the accuracy of the information contained in consumer credit reports and limit the availability of these reports.[113] The Federal Fair and Accurate Credit Transactions Act of 2003 (FFACT), which amended the Federal Credit Reporting Act, focuses primarily on consumer reporting agencies and the use of credit reports and credit scores.[114] FFACT addresses additional issues, such as the procedures a business must set up for consumer claims of identity theft, the ability to sell or transfer debt involving identity theft, what may be printed on a credit- or debit-card receipt, and the credit- or debit-card change-of-address process.[115] Despite Congress's continued efforts to enact legislation combating identity theft, the problem still prevails.

2. State Regulations

In addition to the federal legislation enacted, most states have enacted their own statutes involving identity theft.[116] These statutes,

---

[109] Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. § 6801 (2006)).

[110] *Id.*

[111] Pub. L. No. 91-508, § 602, 84 Stat. 1127 (1970) (codified as amended at 15 U.S.C. §§ 1681–1681x (2006)).

[112] TRW Inc. v. Andrews, 534 U.S. 19, 23 (2001) (citing § 1681(a)(2006)).

[113] *Id.*; § 1681(b) ("It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."); *see also id.* § 1681b (Permissible Purposes of Consumer Reports); *id.* § 1681c (Requirements Relating to Information Contained in Consumer Reports).

[114] Pub. L. No. 108-159, 117 Stat. 1952 (2003)(amending 15 U.S.C. §§ 1681–1681x); *see also* Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237, 269–71 (2004).

[115] §§ 1681–1681x ; *see also* Towle, *supra* note 114.

[116] *See, e.g.*, ALA. CODE §§ 13A-8-190–13A-8-201 (LEXIS through 2010 acts); ALASKA STAT. § 11.46.565 (LEXIS through 2009 1st Session); ARIZ. REV. STAT. ANN. § 13-2008 (LEXIS through the forty-ninth legislature); CAL. PENAL CODE § 530.5-530.8 (LEXIS through 2009–10 Extraordinary Sess.); GA. CODE ANN. §§ 16-9-120–16-9-132 (LEXIS

however, do little more than declare identity theft a crime and outline the punishment. While the language of each state's statutes varies, all state statutes attempt to criminalize the transfer or use of another's personal identifying information.[117] States create different degrees or classes of crime and base such distinctions on a number of factors, including how much information the identity thief possessed,[118] the benefit received or value of the goods received,[119] and who the victim was.[120]

Although most statutes punish only the identity thief, some state statutes impose liability on third parties. For example, a Washington statute imposes a duty on anyone who was involved in the fraudulent transaction to provide all transactional information to the victim upon a written request.[121] In doing so, the Washington Legislature places financial institutions at risk for liability in the event of imposter fraud. With the exception of Washington's statute, however, state regulations on identity theft fail to do more than simply criminalize the act.

E. Lack of Legal Redress Available to Victims of Imposter Fraud on Social Networking Sites

Over the years social networking sites have developed from an innocent, fun method of socializing into today's primary mode of communication for both personal and professional matters.[122] This

through 2009 Sess.); N.J. STAT. ANN. § 2C:21-17 (West 2009); N.Y. PENAL LAW §§ 190.77–190.84 (West, Westlaw through 2009 legislation); TEX. PENAL CODE ANN. § 32.51 (LEXIS through 2009 1st Called Sess.); WASH. REV. CODE ANN. § 9.35.020 (West, Westlaw through 2009 legislation).

[117] *See, e.g.*, ALA. CODE § 13A-8-192 (LEXIS through 2010 acts) ("A person commits the crime of identity theft if, without the authorization, consent, or permission of the victim . . . he or she . . . [o]btains, records, or accesses identifying information . . . ."); N.J. STAT. ANN. § 2C:21-17 (West 2009) ("A person is guilty of an offense if the person . . . [o]btains any personal identifying information pertaining to another person and uses that information, or assists another person in using the information . . . ."); WASH. REV. CODE ANN. § 9.35.020 (West, Westlaw through 2009) ("No person may knowingly obtain, possess, use, or transfer a means of identification or financial information of another person . . . .").

[118] *See, e.g.*, COLO. REV. STAT. § 18-5-903 (LEXIS through 2009 Sess.) (varying the classes for criminal possession of a financial device based on how many devices the thief has).

[119] *See, e.g.*, CONN. GEN. STAT. § 53a-129b–c (LEXIS through 2008 Feb. Sess.) (imposing a Class B felony if the value of the benefit exceeds $10,000 and a Class C felony if the value of the benefit exceeds $5,000).

[120] *See, e.g.*, ARK. CODE ANN. § 5-37-227 (LEXIS through 2009 Sess.) (heightening the penalty if the victim is "an elder person or disabled person").

[121] WASH. REV. CODE ANN. § 9.35.040(1) (West, Westlaw through 2009).

[122] ATTACK INTELLIGENCE RESEARCH CTR., *supra* note 69.

expansion, however, has not been all fun and games. Although the social networking sites are constantly trying to improve their security protections to avoid spammers and hijackers from gaining access, these sites currently operate with limited regulations and legal consequences.[123] The majority of social networking sites, including Facebook and MySpace, have no system in place to verify that users are who they say they are.[124] In turn, social networking sites provide identity thieves with limitless opportunities to perpetrate identity crimes.[125]

Under the Federal Identity Theft and Assumption Deterrence Act and various state identity-theft laws, victims of imposter fraud on social networking sites are able to seek redress by directly pursuing criminal and civil penalties against their imposters.[126] This option, however, is not always available because, before filing a claim, a plaintiff would need to track down the imposter's true identity through the maze of the virtual world, which allows imposters to hide behind IP addresses and pseudonyms.[127] Moreover, even if the victim discovers the impostor's identity, he or she might still have a difficult time recovering damages if the imposter is insolvent. In addition, it is possible that if the court considers the fraudulent profile a mere parody, there may be no legal remedy available.[128]

Apart from the state and federal legislation imposing criminal or civil penalties on identity theft, the current identity-theft legislation is outside the scope of most, if not all, claims of imposter fraud on social networking sites. Although state and federal legislatures have begun enacting laws to combat the prevalence of identity theft, these statutes primarily focus on identity theft in the context of credit or fi-

---

[123] *See, e.g.*, *Privacy*, FACEBOOK, http://www.facebook.com/policy.php?ref=pf (last visited Aug. 14, 2011); *see supra* Part II.C.

[124] Wood, *supra* note 18; *see also* ALADDIN KNOWLEDGE SYSTEMS, *supra* note 69 (describing the potential for an "online nightmare . . . unless a more reliable, trustworthy model of easily connecting an online persona to a true person catches up with social networking sites").

[125] ATTACK INTELLIGENCE RESEARCH CTR., *supra* note 69.

[126] *See supra* notes 103–15 and accompanying text (detailing the federal law criminalizing identity theft); *see also supra* notes 116–21 and accompanying text (detailing state laws criminalizing identity theft).

[127] *See* Evan Brown, *Maryland Court of Appeals Addresses Important Question of Internet Anonymity*, INTERNET CASES BLOG (Mar. 8, 2009), http://blog.internetcases.com/2009/03/08/maryland-court-of-appeals-addresses-important-question-of-internet-anonymity/ (discussing the varying standards jurisdictions use in determining whether to grant a subpoena for the operating service to reveal the identity of the poster).

[128] Wood, *supra* note 18.

nancial fraud.[129] The Federal Credit Reporting Act and FFACT, for example, establish standards for credit reporting and the dissemination of an individual's private information, which is useless to a victim of imposter fraud on social networking sites.[130] Unlike financial institutions and credit-reporting agencies, social networking sites are not subject to any federal or state regulations; thus, they have free reign over how or whether they should monitor and regulate their sites. Victims of imposter fraud on social networking sites should be able to seek redress from the people or institutions that made the crime possible in the first place. Requiring these individuals to directly pursue the perpetrator after the fact does not get at the heart of the problem—preventing imposter fraud from occurring in the first place.

III. NEGLIGENT ENABLEMENT OF IMPOSTER FRAUD: A SOLUTION TO THE PROBLEM OF IMPOSTER FRAUD ON SOCIAL NETWORKING SITES

The common-law tort of negligent enablement of imposter fraud is the most relevant legal mechanism available to victims of imposter fraud, absent action by either state legislatures or Congress that imposes regulations on social networking sites. Although courts generally disfavor this cause of action in the realm of identity theft through financial institutions,[131] courts have yet to examine the tort in the context of imposter fraud on social networking sites. Negligent enablement of imposter fraud could be the saving grace for victims of imposter fraud because it provides victims with legal redress and forces social networking sites to prevent identity theft on their websites in the first place.

A. Common-Law Tort of Negligent Enablement of Imposter Fraud

Plaintiffs largely use the common-law cause of action of negligent enablement of imposter fraud when a financial institution's negligence assists or furthers an imposter's effort to steal their identities.[132] Plaintiffs generally use the tort to hold a financial institution

[129] *See supra* Part II.D (discussing the current regulations in the field of identity theft).

[130] *See supra* notes 111–15 and accompanying text.

[131] *See infra* Part III.A.

[132] *See, e.g.*, Patrick v. Union State Bank, 681 So. 2d 1364, 1365–66 (Ala. 1996) (detailing how a bank's failure to verify the identity of an individual opening an account resulted in an imposter incurring $1,500 worth of debt in the plaintiff's name, which

liable for identity theft that occurred at or with the help of the institution.[133] Although the financial institution was not the actual identity thief, its negligence allowed the identity theft to occur.[134] Victims bring claims of negligent enablement of imposter fraud because identity-theft victims have difficulty receiving compensation for their injuries from their actual imposters.[135]

To establish a claim for negligent enablement of imposter fraud, a plaintiff must, as in all negligence claims, prove duty, breach, causation, and injury.[136] In the context of financial institutions, a plaintiff must show that the financial institution had a duty to protect the plaintiff from identity theft. Then, the plaintiff must show that the defendant negligently enabled the identity theft, thereby breaching the duty owed to the plaintiff and causing damages. Courts and scholars, however, have heavily debated whether a duty exists to prevent imposter fraud or identity theft from occurring to a third party.[137]

Courts throughout the nation have given mixed reviews to negligent enablement of imposter fraud, with some recognizing the cause of action and others refusing to recognize the tort or placing limits on its application. For example, the Supreme Court of Alabama upheld a claim of negligent enablement of imposter fraud in *Patrick v. Union State Bank*.[138] The court discussed the key factors in determining whether a duty existed—foreseeability, the nature of the defendant's activity, the relationship between the parties, and the potential injury or harm.[139] After considering these factors, the court held that banks do in fact have a duty to the public-at-large.[140] A special relationship existed because of "the importance of, and the public trust placed in, the banking industry."[141] The court further held that a special relationship existed because the injury was foreseeable

ultimately resulted in the plaintiff's arrest and incarceration for ten consecutive days).

[133] *See e.g.*, *id.* at 1366–67.

[134] *See id.* at 1367.

[135] Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who's Going to Pay for It?*, 88 MARQ. L. REV. 847, 848 (2005).

[136] RESTATEMENT (SECOND) OF TORTS § 328A (1979).

[137] *See, e.g.*, *Patrick*, 681 So. 2d at 1367–68; Piscitelli v. Classic Residence by Hyatt, 973 A.2d 948, 963 (N.J. Super. Ct. App. Div. 2009); Huggins v. Citibank, N.A., 585 S.E.2d. 275, 277 (S.C. 2003).

[138] *Patrick*, 681 So.2d at 1371–72. The court never explicitly referred to the cause of action as negligent enablement of imposter fraud. *See generally id.*

[139] *Id.* at 1368–69.

[140] *Id.* at 1369.

[141] *Id.*

and the bank was in the best position to prevent the harm from occurring.[142] Subsequent treatment of the holding in *Patrick*, however, is less favorable to recognizing negligent enablement of imposter fraud as a remedy to victims of imposter fraud at financial institutions. Alabama courts have distinguished, limited, and criticized the *Patrick* holding,[143] and courts outside of Alabama have severely limited or rejected it.[144]

Like the Alabama court, the South Carolina Court of Appeals also held a financial institution liable to a third party for failing to follow the procedures.[145] This failure led to the victim's stolen identity.[146] The court held that the bank owed a duty of care to the victim of the identity theft when the victim asked the bank to close the fraudulently opened accounts.[147] The South Carolina Supreme Court, however, later held that South Carolina would not recognize negligent enablement of imposter fraud.[148]

Several state courts expressly refuse to recognize the tort of negligent enablement of imposter fraud. These courts rely on two cases that held that financial institutions have no relationship with, and therefore no duty to, victims of imposter fraud.[149] In *Polzer v. TRW, Inc.*, the New York Intermediate Appellate Court held that New York does not recognize a cause of action for negligent enablement of im-

[142] *Id.* at 1369, 1371.

[143] *See, e.g.*, Flying J Fish Farm v. Peoples Bank of Greensboro, 12 So. 3d 1185, 1194–95 (Ala. 2008) (distinguishing *Patrick* on the fact that the bank was not in the best position to prevent the harm and that the bank intended that the loan-approval policies would protect the bank, not the customer); Smith v. AmSouth Bank, Inc., 892 So. 2d 905, 911 (Ala. 2004) (explaining that although the result may have been the same, the "inquiry in *Patrick* was not properly focused").

[144] *See, e.g.*, Eisenberg v. Wachovia Bank, N.A., 301 F.3d 220, 226 (4th Cir. 2002) (citing *Patrick* as authority contrary to its decision); Guerra v. Regions Bank, 188 S.W.3d 744, 748 (Tex. App. 2006) (refusing to follow *Patrick*); Nicholl v. Nationsbank of Ga., N.A., 488 S.E.2d 751, 753 (Ga. Ct. App. 1997) (limiting *Patrick* to its facts).

[145] Murray v. Bank of Am., 580 S.E.2d 194, 198 (S.C. Ct. App. 2003)

[146] *Id.* at 196–97.

[147] *Id.* at 198.

[148] *See infra* note 152 and accompanying text.

[149] *See, e.g.*, Fargis v. Am. Express Travel Related Servs., No. 1:07-1507-MBS, 2009 U.S. Dist. LEXIS 2398 (D.S.C. Jan. 12, 2009) (holding, a similar position to *Huggins*, that a special relationship that gave rise to a legal duty did not exist between plaintiff and AmEx); Smith v. Citibank, N.A., No. 00-0587-CV-W-1-ECF, 2001 U.S. Dist. LEXIS 25047 (W.D. Mo. Oct. 3, 2001) (holding a, similar position to *Polzer*, that financial institutions do not have a duty to non-customers because a special relationship does not exist).

poster fraud.[150] The court further held that the plaintiffs and the financial institutions do not have a special relationship that gives rise to a traditional claim of negligence.[151] The South Carolina Supreme Court, ignoring the previous appellate decision which held to the contrary, joined New York's rejection of the negligent enablement of imposter fraud claim in *Huggins v. Citibank*.[152] The court held that issuers of credit cards do not have a legal duty to victims of identity theft because the relationship is too attenuated.[153] The court opined that, although the harm is foreseeable, foreseeability alone is not enough to give rise to a duty.[154] The court noted that victims of credit card fraud have remedies available through current state and federal legislation, and although these remedies may not always fully compensate victims of identity theft, the legislature is better equipped to handle this area.[155]

A 2007 opinion from the District of Tennessee, however, criticized *Huggins* and held that a bank has a duty to verify the authenticity and accuracy of a credit account application.[156] The court found that the *Huggins* court's reliance on the absence of a prior business relationship between the victim and the bank was flawed.[157] The determination of whether a duty exists should involve an "examin[ation] [of] all relevant circumstances with an emphasis on the foreseeability of the alleged harm."[158]

In addition to recognizing the tort of negligent enablement of imposter fraud against financial institutions, the New Jersey Appellate Division recently discussed the tort in the employment context. The court addressed whether employers are liable for failing to verify the identity of prospective employees.[159] In *Piscitelli v. Classic Residence by Hyatt*, an immigrant woman used the plaintiff's name and social security number, which she purchased for $800 from an unidentified per-

[150] 256 A.D.2d 248, 249 (N.Y. App. Div. 1997). The court does not explain its reasoning for not recognizing this cause of action. *See id.*

[151] *Id.*

[152] 585 S.E.2d 275, 276 (S.C. 2003).

[153] *Id.* at 277.

[154] *Id.*

[155] *Id.* at 277–78

[156] Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 881–82 (W.D. Tenn. 2007).

[157] *Id.*

[158] *Id.* at 882. The court held that a duty exists because the idea that harm will result from the negligent issuance of a credit card is foreseeable. *Id.*

[159] *See* Piscitelli v. Classic Residence by Hyatt, 973 A.2d 948, 959 (N.J. Super. Ct. App. Div. 2009).

son, to obtain employment as a maid with the defendant.[160] The plaintiff sought to hold the defendant liable for negligently enabling the imposter to become lawfully employed using her information.[161] Although the appellate division recognized that identity theft and harm to an unrelated third-party was reasonably foreseeable when employers fail to verify the identity of their prospective employees, the court nonetheless held that an employer does not have a duty to third parties to verify a prospective employee's identity.[162] Taking into consideration questions of fairness and policy, the court determined that the burden imposed on an employer would be too great and the potential increase in the cost of hiring would be contrary to the public's interest.[163]

Although the claim of negligent enablement of imposter fraud has received less than favorable treatment from the courts in the context of financial institutions and employment, only a few states have addressed the tort thus far.[164] With the continued prevalence of identity theft and the lack of effective solutions, however, the claim of negligent enablement of imposter fraud remains a possible avenue for plaintiffs to seek redress.

B. The Communications Decency Act: A Traditional Bar to Claims Against Social Networking Sites

To hold a social networking site liable for negligent enablement of imposter fraud, a plaintiff must first establish that the CDA's immunity provision does not defeat the claim. Unfortunately, most courts have interpreted § 230 as providing social networking sites with broad immunity insulating these sites from certain civil lawsuits.[165] The case law, however, does not completely foreclose liability for social networking sites for failure to implement reasonable security measures. More recently, courts have begun to recognize that the Internet provides a mode of communication that no longer needs this insulation to thrive, especially in light of the vast amount of harm

[160] *Id.* at 951.

[161] *Id.* at 962–63.

[162] *Id.* at 967 ("[T]he ability to foresee an injury does not in itself establish the existence of a duty.").

[163] *Id.* The court also noted that adopting this new duty would "upset traditional concepts and basic principles dealing with protection and remedies in the field of identity theft" because the legislature has enacted a statute providing victims a remedy through the imposter. *Id.*

[164] Kristin E. Solomon, *Facing Identity Theft: New Victim's Rights Act Imposes New Rules to Protect You*, 12 TENN. B.J. 12, 14 (2004).

[165] *See supra* Part II.C (discussing cases interpreting § 230 as a broad immunity).

facilitated by the Internet over the years.[166] In turn, courts have began to revisit and reinterpret the § 230 immunity provision.[167]

1. Plaintiffs May Sue Social Networking Sites for Negligent Enablement of Imposter Fraud Regardless of the CDA Because the § 230 Immunity Does Not Apply.

When interpreting legislation, courts look to the plain language of the statute and the legislative history.[168] Applying these principles to § 230, it becomes evident that the Act meant to provide protection for those interactive computer services that attempt to screen or block offensive material, not to provide a blanket immunity to those who fail to do anything to screen material.

Congress enacted the § 230 immunity provision as part of Title V of the Telecommunications Act, which is entitled "Obscenity and Violence."[169] Section 230's title is "Protection for private blocking and screening of offensive material" and § 230(c)'s title is "Protection for 'Good Samaritan' blocking and screening of offensive material."[170] In *Doe v. GTE Corp.*, Judge Easterbrook noted that the title is "hardly an apt description if its principle effect is to induce ISPs to do nothing about the distribution of indecent and offensive materials via their service."[171] Rather, one should read the text of the CDA in conjunction with the title.[172] Thus, § 230(c)(1) becomes a "definitional clause" defining those entities that are eligible for immunity under § 230(c)(2)—those interactive computer services that take action to

[166] *See, e.g.*, Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1163 n.15 (9th Cir. 2008) ("[T]he internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations . . . . And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress."). *But see*, Ryan Singel, *FCC Approves Net Neutrality Rule, Now the Fight Begins*, WIRED (Oct. 22, 2009, 1:29 PM), http://www.wired.com/epicenter/2009/10/fcc-net-neutrality/ (discussing the FCC's recently proposed Net Neutrality Rules which will, in part, disallow broadband internet providers to block legal content sent over the internet by users and limit users' ability to run lawful applications of their choice).

[167] *See supra* Part II.C (discussing the recent shift in interpretation of § 230).

[168] *See generally* WILLIAM N. ESKRIDGE ET AL., LEGISLATION, STATUTES AND THE CREATION OF PUBLIC POLICY (West Law School 2007).

[169] Pub. L. No. 104, 110 Stat. 104 (1996) (codified at 47 U.S. § 230 (2006)). Title V is also known as the Communications Decency Act. *Id.*

[170] 47 U.S.C. § 230 (2006).

[171] 347 F.3d 655, 659 (7th Cir. 2003). Judge Easterbrook's analysis in *GTE Corp.* was later adopted in *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist*, 519 F.3d 666, 669–70 (7th Cir. 2008).

[172] *GTE Corp.*, 347 F.3d at 659.

block or screen offensive material.[173] Under such an analysis, interactive service providers that take the "do nothing" approach cannot be immune from all lawsuits against them.

Congress specifically enacted § 230 to overrule *Stratton Oakmont, Inc. v. Prodigy Service, Co.*,[174] which held an interactive computer service liable because of its editing and removal capabilities.[175] The Senate Conference Report further suggests the limitation of the immunity provision by providing that the purpose of the Good Samaritan provisions is to protect interactive computer services from civil liability "for actions to restrict . . . access to objectionable online material."[176] Social networking sites, by not attempting to prevent identity theft, do not fall within in the Good Samaritan provision of § 230.

In addition, social networking sites may be deemed outside the reach of the § 230 immunity provision for enabling identity theft because they are not treated as the publisher or speaker of information. Examining multiple provisions of § 230, one court suggested a three-pronged test to establish who qualifies for immunity.[177] First, the website must be an "interactive service provider;" second, the cause of action must treat the website as a "publisher or speaker" of information; and third, another "information content provider" must have provided the information.[178] In arguing for application of the immunity provision, the first prong—the requirement that the website be an interactive service provider—is easy for a social networking site to prove because the case law explicitly places websites within the definition of an interactive service provider.[179] The third requirement for immunity is also easy to prove because the information at issue is not posted by the social networking site itself. All of the information that a user posts, including profile information, is provided by the user without intermediary editing or screening by the social networking site. This requirement, however, might not be met because the claim at issue in

---

[173] *Craigslist*, 519 F.3d at 670.

[174] S. REP. NO. 104-230, at 194 (1996) ("One of the specific purposes of this section is to overrule *Stratton Oakmont* . . . and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

[175] No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 25, 1995).

[176] S. REP. NO. 104-230, at 194.

[177] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100 (9th Cir. 2009).

[178] *Id.*

[179] *See* Doe v. MySpace, 474 F. Supp. 2d 843, 846 (W.D. Tex. 2007).

this Comment is about the procedures in place for registering, not what the information content provider has posted about the user.

Social networking sites should not receive immunity because they do not meet the second requirement for immunity. The causes of action typically barred under § 230 are defamation and other similar claims related to the actual comments posted by another user of the website.[180] Some plaintiffs have tried to mask their defamatory statement claims as negligence claims; however, the courts have seen through this "tactic" and, instead, have looked to the underlying facts at issue.[181] But, bringing a claim of negligent enablement of imposter fraud is not a tactic to hide a claim about comments made on the site; rather, it is an attempt to hold social networking sites liable for their inadequate procedures. The claim does not relate to a social networking site's capacity as a publisher or as a speaker of its users' content, but rather, to the social networking site's capacity as a provider of the site in the first place. Therefore, § 230 immunity would not cover a claim under a theory of negligent enablement of imposter fraud.

Considering the legislative record for the § 230 amendment, the immunity provision does not apply to claims such as negligent enablement of imposter fraud. As a whole, the CDA immunity was a mix of efforts to regulate material, specifically pornography, available on the Internet, promote freedom of speech on the Internet, and allow ISPs to self-regulate without fear of "publisher liability."[182] While Senator Exon was concerned about the availability of obscene content on the Internet and wanted to protect children and families,[183] Representatives Cox and Wyden wanted to put the pressure on parents to use available filtering software to protect their children.[184]

---

[180] *See, e.g.*, Chi. Lawyers' Comm. for Civil Rights Under Law v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

[181] *See, e.g.*, *Barnes*, 570 F.3d at 1101; Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003).

[182] *See* 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995); *see also* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 52–53 (1996); Emily K. Fritts, *Internet Libel and the Communications Decency Act: How the Courts Erroneously Interpreted Congressional Intent with Regard to Liability of Internet Service Providers*, 93 KY. L.J. 765, 774–75 (2004).

[183] 141 CONG. REC. 18,046 (1994) (statement of Sen. Exon). In 1994, Senator Exon proposed an amendment to the CDA which would "update[] [the CDA]for the digital world of the future." *Id.* Senator Exon aimed "to protect children from being exposed to obscene, lewd, or indecent messages." *Id.*

[184] 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Wyden) ("[W]e believe that parents and families are better suited to guard the portals of cy-

The emphasis on obscenity throughout the legislative history, in addition to the text of the Act itself, suggests that the immunity provision would not extend to claims for inadequate procedures that facilitate imposter fraud.[185]

In addition, the § 230 immunity should be limited for policy reasons. Imposter fraud has the potential to be extremely harmful and efforts to help combat this overwhelmingly prevalent crime would be in accord with public policy. Furthermore, imposing liability on social networking sites does not frustrate the findings and policies at the foundation of the CDA.[186] Encouraging social networking sites to have effective verification measures does not limit the ability of these sites to be a "forum for true diversity of political discourse, . . . cultural development, and . . . intellectual activity," or the ability of these sites to be relied on; rather, it furthers these ideas by ensuring that the speaker is who the speaker claims to be.[187] Allowing liability in this situation also does not hinder the "continued development of the Internet" or the preservation of the "vibrant and competitive free market," but rather it encourages it.

2. In the Alternative, Congress Should Amend the CDA to Permit Liability of Social Networking Sites for Enabling Identity Theft

If courts are unwilling to read the CDA immunity provision to exclude liability for failure to implement appropriate verification measures, Congress should amend the CDA to limit the current law's blanket immunity. To hold social networking sites responsible for facilitating identity theft through their websites, Congress should amend the current immunity provision to read, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider, *except for the purposes of preventing identity theft*."

This proposed amendment would prevent a social networking site from claiming § 230 immunity when the site's ineffective preven-

berspace and protect our children than our Government bureaucrats. Parents can get relief now from the smut on the Internet by making a quick trip to the neighborhood computer store where they can purchase reasonably priced software that blocks out the pornography on the Internet."); *see also* Meyers, *supra* note 76, at 172.

[185] *See* 141 CONG. REC. H8469–71 (daily ed. Aug. 4, 1995). Every Representative that spoke on the proposed § 230 amendment discussed it in reference to the problem of child pornography. *Id.*

[186] *See supra* notes 82–85 and accompanying text (listing the policy goals of the CDA).

[187] 47 U.S.C. § 230(a)(3), (5) (2006).

tative measures allow an imposter to create an account in another's name. By creating a specific exception to the current rule, this proposal would still protect social networking sites from liability for every word, sentence, or picture posted on the site. Therefore, social networking sites would only be subject to liability if they neglect to maintain reasonable procedures to prevent imposter fraud.

The CDA presents a hurdle to a plaintiff seeking redress against social networking sites because courts have often granted these websites blanket immunity against lawsuits resulting from information posted on their website. In doing so, courts effectively established the Internet as a place where anything goes. In recent years, courts have reinterpreted the immunity provision more narrowly, which gives hope to plaintiffs who seek redress for imposter fraud on social networking sites. In the alternative, Congress should explicitly amend the provision to allow for such liability. The expansive growth and advancement of the Internet calls for the courts and Congress to take a second look at the protections that they provided when the Internet initially began.

C. Applying the Cause of Action of Negligent Enablement of Imposter Fraud to Social Networking Sites

The tort of negligent enablement of imposter fraud, although novel, remains a viable cause of action for victims of imposter fraud on social networking sites. In establishing the tort of spoliation,[188] the California Court of Appeal, in *Smith v. Superior Court*, quoted Prosser and Keeton:

> New and nameless torts are being recognized constantly, and the progress of the common law is marked by many cases of first impression, in which the court has struck out boldly to create a new cause of action, where none has been recognized before . . . . The law of torts is anything but static, and the limits of its development

[188] The tort of spoliation holds an individual who "intentionally destroys, mutilates, or alters evidence, and thereby interferes with a person's prospective or actual civil action against either the spoliator or a third person, [] liable in tort to that person." Thomas G. Fischer, Annotation, *Intentional Spoliation of Evidence, Interfering with Prospective Civil Action, as Actionable*, 70 A.L.R.4th 984, § 2. Although not every state recognizes this independent tort, over the past 10 years or so several states, such as Indiana and Ohio, do recognize spoliation as a tort claim. *Id.* The elements of the tort can vary, but one court requires: (1) "pending or probable litigation involving plaintiff," (2) "knowledge on the part of defendant that litigation exists or is probable," (3) "willful destruction of evidence by defendant designed to disrupt the plaintiff's case," (4) "disruption of plaintiff's case," and (5) "damages proximately caused by the defendant's acts." Smith v. Howard Johnson Co., 615 N.E.2d 1037, 1038 (Ohio 1993).

> are never set. *When it becomes clear that the plaintiff's interests are entitled to legal protection against the conduct of the defendant*, the mere fact that the claim is novel will not of itself operate as a bar to remedy.[189]

Victims of imposter fraud are undoubtedly entitled to protection against the lack of action by the social networking sites. Expanding the tort of negligent enablement of imposter fraud to cover social networking sites would not only provide victims with a realistic remedy, but would also encourage social networking sites to increase security and regulating measures and ultimately decrease the instances of imposter fraud.

The tort of negligent enablement of imposter fraud is similar to the traditional tort of negligence. Negligent conduct is characterized as that which "falls below the standard established by law for the protection of others against unreasonable risk of harm," and the standard is "that of a reasonable man under like circumstances."[190] To establish a cause of action for negligent enablement of imposter fraud, the plaintiff must show the following elements: (1) the defendant owed a duty of care to the plaintiff to prevent or attempt the prevent imposter fraud from occurring, (2) the defendant breached that duty by failing to attempt to prevent imposter fraud from occurring, (3) the defendant's failure caused injury to the plaintiff, and (4) the plaintiff suffered an injury for which a court can award damages.[191] The first and most difficult element to prove is the existence of a duty. The plaintiff must convince the court to impose a duty on social networking sites to act reasonably when allowing users to register.

1. Social Networking Sites Should Have a Duty to Implement Reasonable Protections Against Imposter Fraud

Social networking sites should have a duty to third parties to implement reasonable registration procedures protecting against imposter fraud. Defined, a duty is "an obligation, to which the law will give recognition and effect, to conform to a particular standard of conduct toward another."[192] The general rule is that no legal duty ex-

[189] 151 Cal. App. 3d 491, 495–96 (Ct. App. 1984) (quoting W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 1, at 3–4 (4th ed. (1971))).

[190] RESTATEMENT (SECOND) OF TORTS § 282 (1965).

[191] *See id.* § 281 (detailing the elements of a cause of action for negligence).

[192] W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 53 (W. Page ed., 5th ed. 1984).

ists to prevent harm to third parties.[193] But, courts do impose a duty on third parties in the presence of special circumstances or relationship. When determining whether a duty exists, courts often consider questions of policy and fairness, including the type of injury or harm, the foreseeability of the injury or harm, the relationship between the parties, and other public policy and social considerations.[194]

Although foreseeability does not establish a duty in itself, the fact that the harm is foreseeable is a "crucial element" given significant consideration.[195] Courts generally use foreseeability to limit a tortfeasor's liability; however, it has also been used to create a legal duty.[196] Interpreting Judge Cardozo's language in *Palsgraf v. Long Island Railroad*, William Prosser stated, "Negligence must be a matter of some relation between the parties, some duty, which could be founded only on foreseeability of some harm to the plaintiff in fact injured."[197] Courts have adopted foreseeability as the central element to establish a legal duty.[198]

In the context of social networking sites, it is reasonably foreseeable that the relaxed "honor code" mechanisms in place for registration allow an individual to register for these sites as someone else, which results in a myriad of potential harms. The absence of any form of verification creates a limitless opportunity for fraud. To create an account on a social networking site, an imposter simply needs to create a fake email address to which the account will be linked and enter a few basic personal facts.[199] Anyone who has the slightest bit of personal information available on the Internet is only a few clicks away from an imposter creating an account in his or her

---

[193] RESTATEMENT (SECOND) OF TORTS § 315(b) (1965).

[194] *See, e.g.*, Key v. Compass Bank, 826 So. 2d 159, 170 (Ala. Civ. App. 2001); Chi Lap Yan v. Ill. Farmers Ins. Co., No. 1:03-CV-1980-SEB-JPG, 2005 U.S. Dist. LEXIS 33819, at *11 (S.D. Ind. Sept. 2, 2005) (holding that to determine the existence of a duty, three factors are balanced: (1) the relationship between the parties, (2) the reasonable foreseeability of harm to the person injured, and (3) public concerns); Piscitelli v. Classic Residence by Hyatt, 973 A.2d 948, 966 (N.J. Super. Ct. App. Div. 2009).

[195] *Piscitelli*, 973 A.2d at 966 (citing Carter Lincoln-Mercury, Inc. v. EMAR Grp., Inc., 638 A.2d 1288, 1294 (N.J. 1994)).

[196] Steffen Nolte, *The Spoliation Tort: An Approach to Underlying Principles*, 26 ST. MARY'S L.J. 351, 376 (1994).

[197] William L. Prosser, Palsgraf *Revisited*, 52 MICH. L. REV. 1, 5 (1953). Judge Cardozo first referenced foreseeability of harm to the plaintiff in the context of duty in *Palsgraf v. Long Island Railroad*, 162 N.E. 99, 101 (N.Y. 1928).

[198] Nolte, *supra* note 196 (listing several courts relying on foreseeability as the primary element in determining duty).

[199] *See supra* note 69–70 and accompanying text (discussing how imposters can easily generate a profile in someone else's name).

name. Although the harm from imposter fraud is highly foreseeable, the inquiry as to whether a duty should be imposed does not stop there.[200]

Although a traditional relationship does not exist between a victim of imposter fraud and a social networking site, a special relationship nonetheless exists, which gives another reason for courts to impose a duty. The only connection between the parties is likely to be through the imposter. One scholar, however, suggests that this is enough: "Although the victimized individual is not a bank 'customer' in the traditional sense, the financial institution acts under the presumption that the named individual is the 'customer' when the imposter presents the named individual's identifying information."[201] Similarly, a social networking site operates as if the victim is a user or a member until notified about the fraud. Therefore, the "third-party" victim has a pseudo-relationship with the social networking site.

Imposing a duty is also appropriate because such a duty would not be too burdensome on social networking sites. Although the harm may be foreseeable, courts are not likely to impose a duty if the imposition will be unfair, either physically or financially.[202] Verification technology currently exists and a few social networking sites, such as eHarmony.com and Funky Sexy Cool, have started to offer verification as an option to its users.[203] IDology and RelyID currently of-

[200] Courts place varying emphasis on the foreseeability requirement. *See, e.g.*, Patrick v. Union State Bank 681 So. 2d 1364, 1368 (Ala. 1995) (holding that the ability to foresee the injury is the "key factor"); Carter Lincoln-Mercury, Inc. v. EMAR Grp. Inc., 638 A.2d 1288, 1294 (N.J. 1994) (noting that foreseeability is a "crucial element" but not the only element); Huggins v, Citibank, 585 S.E.2d 275, 277 (S.C. 2003) ("[F]oreseeability alone does not give rise to a duty."); Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) ("[A court] must examine all the relevant circumstances with an emphasis on the foreseeability of the alleged harm.").

[201] Heather M. Howard, *The Negligent Enablement of Imposter Fraud: A Common-Sense Common Law Claim*, 54 DUKE L.J. 1263, 1286–87 (2005). This approach is similar to that taken by the court in *Patrick*. *See* Patrick, 681 So. 2d at 1369 ("The fact that the relationship defies common categorization does not mean that there is no relationship.").

[202] *See, e.g.*, Piscitelli v. Classic Residence by Hyatt, 973 A.2d 948, 967 (N.J. Super. Ct. App. Div. 2009)

[203] Zack Martin, *Social Networking Sites Have Little to No Identity Verification*, CR80 NEWS (Mar. 31, 2008), http://www.cr80news.com/2008/03/31/social-networking-sites-have-little-to-no-identity-verification; *see also Trulioo Launches Internet ID Verification System*, VILLAGE GAMER (Sept. 1, 2009), http://www.villagegamer.net/2009/09/01/trulioo-launches-internet-id-verification-system [hereinafter *Trulioo Launches*].

fer identification- and age-verification technology.[204] IDology's software takes information provided by the consumer, such as name, year of birth, and residence zip code, and searches through public data records to verify the identity of the consumer.[205] IDology also offers advanced software, which generates multiple choice questions from the information provided, including questions about historical addresses, people the user knows, and cars the user has owned.[206] Similarly, RelyID's technology checks public record databases and comes back with a multiple-choice quiz. Then, upon passing the quiz, the user becomes verified.[207] This technology is limited in the instance of minors because they lack public data.[208] A solution to this problem, however, could be to require a parent—verified through the public record searching technology—to confirm that his or her child is who the child claims to be.[209] In addition, another available software verifies a person's identity by asking questions to that person's "friends" or contacts on the social networking site.[210] A concern, however, is that these verification systems can be costly.[211] Although expensive at the moment, the cost can likely be reduced as the demand for verification systems increases (because of the threat of potential liability). In addition, social networking sites can deflect the cost of the system to the users or advertisers.

Furthermore, courts should impose a duty on social networking sites because such a duty is in the best interest of the public. Courts look to a variety of public policy interests, such as who is in the best position to prevent the harm, to determine if imposing a duty is important.[212] In this situation, social networking sites are the first and the last line of defense against imposter fraud. Apart from preemp-

---

[204] *See Solutions for ID verification*, IDOLOGY, http://www.idology.com/solutions/solutions (last visited Mar. 16, 2011); *Products*, RELYID, http://www.relyid.com/products.html (last visited Mar. 16, 2011).

[205] John Dancu, *Using Identity and Age Verification within Social Networking Sites*, IDOLOGY 1 (July 21, 2008), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/IDology_ISTTFTAB_submission.pdf.

[206] *Id.*

[207] Martin, *supra* note 203.

[208] *Id.*

[209] *Id.*

[210] *Trulioo Launches*, *supra* note 203. The Trulioo technology is currently available on Facebook as an optional application. *Id. See* TRULIOO, http://trulioo.com (last visited Feb. 13, 2011).

[211] Martin, *supra* note 203. IDology charges thirty-seven cents per verification. *Id.*

[212] *See, e.g.*, Piscitelli v. Classic Residence by Hyatt, 973 A.2d 948, 114 (N.J. Super. Ct. App. Div. 2009).

tively creating a profile on all social networking sites, individuals can do very little to prevent imposter fraud. In addition, often a victim does not realize that someone has been "posing" as him or her for quite a while and by the time the victim discovers the fraud, the damage has already been done. Social networking sites, however, are in a prime position to prevent imposters from having the opportunity to commit this crime. The value of protecting individuals' identity, especially when identity theft is on a rapid rise, is likely to trump any public policy considerations to the contrary.

2. The Social Networking Site's Failure to Implement Reasonable Registration Procedures Causes Imposter Fraud

Social networking sites should be liable against victims of imposter fraud on their sites because their failure to reasonably regulate how members register for the site causes imposter fraud to occur. In proving the element of causation, a plaintiff will need to show that the site's breach of the duty to impose reasonable procedures preventing imposter fraud caused the plaintiff's injury.[213] Causation is established if the defendant's conduct was a "substantial factor in bringing about the harm."[214] To prevent extensive liability, an individual is not held liable for negligent conduct if the conduct was too far removed from the injury.[215] Generally, courts do not recognize causation when no one could reasonably foresee the injury.

In this context, a social networking site's lack of appropriate procedures for registration enables the imposter to create a false profile. As discussed above, website operators can reasonably foresee that without a verification system or procedure in place, imposter fraud could occur on the site. Thus, if reasonable procedures were in place for registration on the social networking site, imposter fraud would not occur.[216]

[213] RESTATEMENT (SECOND) OF TORTS § 430 (1965).

[214] *Id.* § 431.

[215] Ultramares Corp. v. Touche, 174 N.E. 441, 444 (N.Y. 1931) (limiting liability in order to avoid creating "liability in an indeterminate amount for an indeterminate time to an indeterminate class").

[216] If an instance of imposter fraud by chance occurs despite the site's procedures, the site would not be liable if the procedures in place were reasonable.

3 The Lack of Reasonable Procedures Harms Victims of Imposter Fraud

A victim of imposter fraud on social networking sites suffers injury as a result of the site's negligence. Although the specific injuries vary between plaintiffs, victims of imposter fraud, just like victims of traditional identity theft, have the potential to suffer a wide array of harm.[217] Damages could stem from money and time spent clearing one's name to emotional distress from the incident.[218] The purpose of damages is to "punish wrongdoers and deter wrongful conduct,"[219] and providing damages in this scenario unquestionably punishes social networking sites for their neglect and deters similar neglect in the future.

IV. CONCLUSION

Identity theft has been an established crime for some time; however, it has recently become one of the fastest-growing crimes and concerns among Americans.[220] With this has come the development of a new form of identity theft—imposter fraud on social networking sites. Today, the information needed to assume another's identity is readily available on the Internet. Easy access to important information on the Internet, combined with the lack of verification procedures on social networking sites, creates limitless opportunities for fraud. Skilled identity thieves and innocent, computer-savvy youngsters can pose as someone else on these websites to play a harmless prank on friends, or even worse, to cause serious harms to their victims.

Both Congress and state legislatures criminalized identity theft, which resulted in either monetary fines or incarceration.[221] The complexities of the Internet, however, make actually finding the perpetrator very difficult. Therefore, plaintiffs should be able to turn to another source of the crime to obtain relief—the social networking sites themselves. The CDA has traditionally insulated these sites from liability for negligence-based claims such as defamation, but an analysis of more recent interpretations of the CDA suggests that courts are re-thinking this blanket immunity. Given this recent change in direction, a court addressing a plaintiff's claim against a social networking

[217] *See supra* Part II.B.

[218] *See supra* note 74 and accompanying text.

[219] RESTATEMENT (SECOND) OF TORTS § 901(c) (1965).

[220] *See supra* Part II.B.

[221] *See supra* Part II.D.

site for enabling imposter fraud because of a failure to implement reasonable registration procedures should read the CDA to allow such a claim because the site would not be treated as the publisher or speaker of the content. In the alternative, the legislature should amend the CDA to allow for an exception for preventing imposter fraud and identity theft.

Although met with skepticism in some courts, negligent enablement of imposter fraud is the most appropriate legal mechanism to combat imposter fraud on social networking sites. A plaintiff attempting to use this tort will need to show that the social networking site owed a duty to the public-at-large to implement reasonable registration procedures and, by failing to do so, caused injury or damages. Expanding this tort to the context of social networking sites affords victims of imposter fraud a method of relief and forces social networking sites to take proactive measures to prevent plaintiff imposter fraud on their sites in the first place. The risk of liability will ultimately create a safer Internet without hindering its positive aspects.