TOURO LAW
Touro College Jacob D. Fuchsberg Law Center

Touro Law Review

Volume 29 | Number 2 Article 12

October 2013

Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation

Maksim Reznik

Follow this and additional works at: http://digitalcommons.tourolaw.edu/lawreview


Part of the Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Reznik, Maksim (2013) "Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation," *Touro Law Review*: Vol. 29: No. 2, Article 12.
Available at: http://digitalcommons.tourolaw.edu/lawreview/vol29/iss2/12

This Comment is brought to you for free and open access by Digital Commons @ Touro Law Center. It has been accepted for inclusion in Touro Law Review by an authorized administrator of Digital Commons @ Touro Law Center. For more information, please contact ASchwartz@tourolaw.edu.

Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation

Cover Page Footnote
29-2

This comment is available in Touro Law Review: http://digitalcommons.tourolaw.edu/lawreview/vol29/iss2/12

IDENTITY THEFT ON SOCIAL NETWORKING SITES: DEVELOPING ISSUES OF INTERNET IMPERSONATION

Maksim Reznik[*]

I. INTRODUCTION

In New Jersey, a woman was prosecuted for identity theft after creating a fake Facebook profile that depicted her ex-boyfriend, a narcotics detective, as a sexual deviant and a drug addict.[1] Similarly, in California, a teenager who stole his classmate's Facebook password to post sexually explicit material about the victim was sentenced to a period not to exceed one year in a juvenile detention center.[2] This Comment focuses on the dangers of social media sites when a person gains access to another's online account through two different methods: (1) stealing the third party's password,[3] or (2) creating a completely fake profile and subsequently impersonating that person.[4]

Social networking sites have become an integral part of how our society interacts on a daily basis.[5] Facebook, the current leader in

---

[*] J.D. Candidate 2013, Touro College Jacob D. Fuchsberg School of Law; B.A. 2010, University of Massachusetts, Amherst. I would like to thank my friends and family for supporting me during the journey of law school and life. I would also like to thank the *Touro Law Review* and the Touro Law faculty for making the publication of this article a possibility.

[1] Mark Hansen, *NJ Woman Can Be Prosecuted over Fake Facebook Profile, Judge Rules*, A.B.A. J. (Nov. 4, 2011), http://www.abajournal.com/news/article/woman_can_be_prosecuted_over_fake_facebook_profile_judge_rules; *see* FACEBOOK, http://www.facebook.com (last visited Nov. 19, 2012).

[2] *In re* Rolando S., 129 Cal. Rptr. 3d 49, 52 (Ct. App. 2011).

[3] *See id.* (discussing a case where a teenager received the password to a fellow classmate's email account by means of an unsolicited text message and used this information to access the classmate's Facebook account).

[4] *See* Draker v. Schreiber, 271 S.W.3d 318, 320-21 (Tex. App. 2008) (illustrating a case in which two students created a fake website profile of their principal on MySpace.com).

[5] Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Social networking sites are "web-based services that allow individuals to . . . construct a public or

Published by Digital Commons @ Touro Law Center, 2013

social networking sites, has approximately eight hundred and forty-five million active users,[6] and that number is expected to exceed one billion by the end of 2012.[7] Recent studies show that eighty-five percent of college students spend a weekly average of 6.2 hours on Facebook.[8] Twitter,[9] which emerged in 2006 as a way to send status updates via text messages, currently has 200 million registered accounts, and experts expect that number to reach 900 million by the end of 2012.[10] It can safely be assumed that social media sites will continue to grow and provide services for millions of individuals and companies.

Such excessive growth of social media sites has led to an increasing number of Internet impersonation cases in the United States.[11] This Comment focuses mainly on criminal liability for perpetrators of Internet impersonation, as opposed to the civil context, in which victims can sue perpetrators in tort.[12] The purpose of this Comment is to identify how states are actively attempting to prevent online impersonation and to propose a federal statute to combat online impersonation. This statute is based upon California and New York statutes,[13] but also explicitly applies to the two

---

semi-public profile within a bounded system." *Id.* Users then "articulate a list of other users with whom they share a connection, and . . . view and traverse their lists of connections . . . made by others within the system." *Id.*

[6] Anson Alexander, *Facebook User Statistics 2012 [Infographic]*, ANSON ALEX (Feb. 20, 2012), http://ansonalex.com/infographics/facebook-user-statistics-2012-infographic/.

[7] Priit Kallas, *Social Media Trends 2012: More Than 1 Billion People Using Facebook*, DREAM GROW (Oct. 20, 2011), http://www.dreamgrow.com/social-media-trends-2012-more-than-1-billion-people-using-facebook/.

[8] Jamison Barr & Emmy Lugus, *Digital Threats on Campus: Examining the Duty of Colleges to Protect Their Social Networking Students*, 33 W. NEW ENG. L. REV. 757, 761 (2011).

[9] TWITTER, http://www.twitter.com (last visited Nov. 19, 2012).

[10] Shea Bennett, *Twitter on Track for 500 Million Total Users by March, 250 Million Active Users by End of 2012*, MEDIA BISTRO (Jan. 13, 2012), http://www.mediabistro.com/alltwitter/twitter-active-total-users_b17655.

[11] Bradley Kay, Article, *Extending Tort Liability to Creators of Fake Profiles on Social Networking Websites*, 10 CHI.-KENT J. INTELL. PROP. 1, 3 (2010).

[12] *Id.* at 17 ("The causes of action for misappropriation of name or likeness and violation of right of publicity have been extended to acts committed over the Internet.").

[13] *See* N.Y. PENAL LAW § 190.25(4) (McKinney 2008) ("A person is guilty of criminal impersonation . . . when he . . . [i]mpersonates another by communication by [I]nternet website or electronic means with intent to obtain a benefit or injure or defraud another, or by such communication pretends to be a public servant in order to induce another to submit to such authority or act in reliance on such pretense."); CAL. PENAL CODE § 528.5 (West 2011) (setting forth that "any person who knowingly and without consent credibly impersonates

methods of Internet impersonation within the statutory language.[14] Section II discusses the emerging nationwide problem of Internet impersonation and provides examples of the two methods of online impersonation. Section III explains how certain states are attempting to solve the problem of Internet impersonation. Finally, section IV proposes solutions to limit the negative effects of online impersonation, including an ideal statute that the federal government and states should adopt when dealing with this issue.

II. METHODS TO PERPETRATE IDENTITY THEFT ON SOCIAL MEDIA SITES

Identity theft on the Internet can arise in two similar yet distinct ways. The more common scenario of identity theft on the Internet arises when the perpetrator creates a fictitious profile of the victim and subsequently uses that identity for online communications.[15] The second method occurs when the perpetrator steals a victim's password or indirectly gains access to a victim's social media account and then impersonates the victim by using that account.[16]

A. Creating a Fake Social Media Site Profile

Only a small number of states contain a statute explicitly referring to Internet impersonation.[17] In these states, the possible

---

another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense").

[14] *See* Kay, *supra* note 11 (discussing cases in which an individual creates a fake profile); *see also In re Rolando S.*, 129 Cal. Rptr. 3d at 52 (involving a case where a teenager stole his classmate's password).

[15] Kay, *supra* note 11.

[16] *See, e.g.*, *In re Rolando S.*, 129 Cal. Rptr. 3d at 52 ("Appellant used the victim's email password and account to gain access to her Facebook account, where he posted, in her name, prurient messages on two of her male friends' pages (walls) and altered her profile description in a vulgar manner.").

[17] *See* N.Y. PENAL LAW § 190.25(4) (establishing when an individual is liable for criminal impersonation); CAL. PENAL CODE § 528.5 (discussing the behavior that amounts to Internet impersonation); TEX. PENAL CODE ANN. § 33.07 (West 2011) ("A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to: (1) create a web page on a commercial social networking site or other Internet website; or (2) post or send one or more messages on or through a commercial social

outcome of a case in which a perpetrator creates a fake profile to the detriment of the victim will be clear simply by reading the language of the state's statute. Conversely, the potential results of such cases in states in which statutes are silent on issues of Internet impersonation will not be as clear, and furthermore, may lead to jurisdictional splits concerning this emerging issue.[18]

A premier example of creating a fake social media site profile to defraud or otherwise harm the victim comes from a case in New Jersey.[19] The case involves Dana Thornton, a woman who created a fake Facebook profile for her ex-boyfriend, a narcotics detective.[20] In the detective's fake Facebook profile, Thornton posted that the detective used drugs, hired prostitutes, and had herpes, including statements such as, "I'm an undercover narcotics detective that gets high every day."[21] Thornton's attorney argued that the case should be dismissed because there was no New Jersey identity theft statute including Internet impersonation.[22] The judge, however, refused to dismiss the case because "the law is 'clear and unambiguous' . . . and does not specify the 'means' by which the injury could occur."[23]

Although the judge decided not to dismiss the case, it "could be difficult to prosecute [Thornton] because of the way the New Jersey law is written."[24] Under the New Jersey statute, a person is guilty of identity theft if the person "impersonates another or assumes a false identity and does an act in such assumed character or false identity for the purpose of obtaining a benefit for himself or another or to injure or defraud another."[25] The memorandum in support of the bill for the New Jersey identity theft statute states that "personal identifying information includes name, address, telephone number,

networking site or other Internet website, other than on or through an electronic mail program or message board program.").

[18] Hansen, *supra* note 1 (paraphrasing Bradley Shear, a "lawyer who specializes in online issues," who said that New York and California are leading the way for Internet impersonation cases and that he "expects to see more cases like this one in the near future" in other states).

[19] *Id.*

[20] *Id.*

[21] Ben Horowitz, *Judge Rules Case of Belleville Woman's Fake Facebook Page Can Proceed*, NJ.COM (Nov. 2, 2011), http://www.nj.com/news/index.ssf/2011/11/judge_rules_case_of_fake_faceb.html.

[22] Hansen, *supra* note 1.

[23] Horowitz, *supra* note 21.

[24] Hansen, *supra* note 1.

[25] N.J. STAT. ANN. § 2C: 21-17 (West 2005).

social security number, place of employment, employee identification number, demand deposit account number, savings account number, credit card number and mother's maiden name."[26]

Evidently, the law is not as "clear and unambiguous" as the judge presiding over Dana Thornton's case presumed it to be.[27] In fact, a thorough examination of the legislative intent behind the New Jersey statute of identity suggests that the New Jersey Legislature never intended its identity theft statute to encompass Internet impersonation.[28] The summary of the bill provides that the conduct must satisfy three elements to rise to the level of a criminal offense: (1) "obtaining and using personal identifying information" as described in the bill; (2) absence of consent to obtain and use the identifying information; and (3) an "intent[ion] to obtain a benefit."[29] Thornton clearly satisfied the first two elements when she used her ex-boyfriend's name for the Facebook profile without his consent.[30] However, there is potential for confusion and ambiguity with respect to the third element.[31] The term "benefit" as defined by the statute "means, but is not limited to, any property, any pecuniary amount, any services, any pecuniary amount sought to be avoided or any injury or harm perpetrated on another where there is no pecuniary value."[32] Because of the absence of a pecuniary interest, the only substantive argument that the "benefit" element was satisfied was that Thornton caused a non-pecuniary "injury or harm" to her ex-boyfriend; however, neither the bill nor the statute gives a definition or any assistance in interpreting what constitutes a non-pecuniary "injury or harm."[33]

In a preliminary hearing, the judge refused to dismiss the case because he believed that Thornton's impersonation "allegedly

---

[26] Governor's Conditional Veto Message, Bill nos. 2414, 1638 and 2456, 2005 Main Volume (N.J. 2005), *available at* N.J. STAT. ANN. § 2C: 21-17.

[27] Horowitz, *supra* note 21.

[28] *See* Governor's Conditional Veto Message, Bill no. 2414 (stating that personal information be obtained and used without authorization and with intent to obtain a benefit in order to constitute a criminal offense).

[29] *Id.*

[30] Horowitz, *supra* note 21.

[31] *See* Governor's Conditional Veto Message, Bill no. 2414 (requiring "the intent to obtain a benefit").

[32] N.J. STAT. ANN. § 2C: 21-17 (West 2005).

[33] *Id.*; Governor's Conditional Veto Message, Bill no. 2414.

'injured' the detective's reputation," stating that the law "does not specify the 'means' by which the injury could occur."[34] The judge did not, however, mention that the law failed to specify what type of non-pecuniary "injury or harm" was necessary or what extent the non-pecuniary "injury or harm" must be.[35] Only with the broadest interpretation of the statute can a reasonable person conclude that Thornton's statement on her ex-boyfriend's fake Facebook profile is sufficient to satisfy the non-pecuniary harm or injury requirement under the benefit element.

Nevertheless, the judge "refused to dismiss" Thornton's case and charged her with identity theft.[36] The court that will adjudicate this case will potentially run into similar difficulties in analyzing the New Jersey identity theft statute, as the California court did in analyzing the California identity theft statute in *In re Rolando S.*[37] In *In re Rolando S.*, a juvenile defendant "gain[ed] access to [the victim's] Facebook account," and "posted, in her name, prurient messages on two of her male friends' pages (walls) and altered her profile description in a vulgar manner."[38] The California Court of Appeals and the parties to the litigation applied California's traditional identity theft statute.[39] Under that statute, the perpetrator is guilty if he "willfully obtains personal identifying information . . . of another person, and uses that information for any unlawful purpose . . . without the consent of that person."[40] Rolando argued that his conduct did not satisfy an unlawful purpose as required under the statute.[41] The court analyzed the statute's legislative history to determine what type of conduct falls under "any unlawful purpose" in light of Rolando's argument that the term "unlawful purpose" was

---

[34] Horowitz, *supra* note 21.

[35] *See* N.J. STAT. ANN. § 2C: 21-17 (defining "benefit," but failing to provide a definition for "injury or harm").

[36] Horowitz, *supra* note 21.

[37] 129 Cal. Rptr. 3d 49 (Ct. App. 2011). The court went through a lengthy discussion in order to successfully apply an Internet impersonation scenario to the outdated identity theft statute, which was silent on Internet impersonation. *Id.* at 55-56.

[38] *Id.* at 52. One such comment made by the defendant under the victim's name on a male classmate's wall was as follows: "When we were dating we should have had sex. I always thought you had a cute dick, maybe we can have sex sometime." *Id.* at 52 n.2 (internal quotation marks omitted).

[39] *Id.* at 51-52.

[40] CAL. PENAL CODE § 530.5 (West 2011).

[41] *In re Roland S.*, 129 Cal. Rptr. 3d at 53, 55.

ambiguous.[42]

Through a lengthy and nebulous opinion, the California Court of Appeals ultimately determined that the legislature intended "unlawful purpose" to include acts prohibited by common law, such as intentional civil torts.[43] The court held that Rolando's messages on the victim's Facebook profile constituted libel, which is an intentional civil tort, and therefore satisfied the statutory language of California's identity theft statute.[44] The potential issues a New Jersey court may face in determining what type of "harm or injury" is sufficient for the New Jersey identity theft statute is analogous to the dispute in *In re Rolando S.* concerning what satisfied an "unlawful purpose" under the California identity theft statue. In light of *In re Rolando S.*, California immediately enacted a statute that specifically made identity theft on the Internet illegal in order to prevent future ambiguity.[45]

The New Jersey legislature also has acted to amend New Jersey's identity theft statute to completely bar Internet impersonation. The bill, which has passed the Assembly, is currently before the Senate.[46] The amended statute will undoubtedly clarify the ambiguities that exist in New Jersey's identity theft statute concerning Internet impersonation, but what effect will its enactment have on Dana Thornton's case? Thornton's attorney argued that the amendment of the law is exactly why "there was nothing illegal in Thornton's alleged postings."[47] Alternatively, the prosecutor, Robert Schwartz, argued that the amendment "is merely 'a clarification' of current law," and that "[i]n no way are [the legislators] saying electronic communication has been excluded" under the current statute, and in "[n]o way did the Legislature ever intend for Ms. Thornton to get away with this kind of conduct."[48]

For the reasons discussed above, there is a possibility that the court will hold that the language in the outdated identity theft statute is too broad to include Thornton's actions as illegal. In that scenario,

---

[42] *Id.* at 55-56.
[43] *Id.* at 56-57.
[44] *Id.* at 57-58.
[45] *See* CAL. PENAL CODE § 528.5 (West 2011) (criminalizing Internet impersonation).
[46] Horowitz, *supra* note 21; *see also* Assemb. 2105, 215th Leg. (N.J. 2012).
[47] Horowitz, *supra* note 21.
[48] *Id.* (internal quotation marks omitted).

there must be a determination on whether the amended statute could retroactively apply to Dana Thornton.[49] Under both the New Jersey and Federal Constitutions, however, a legislative body is prohibited form enacting "ex post facto" laws.[50] An "ex post facto" law is defined as "any statute which makes a prior act, that was innocent when committed, a crime, which makes punishment for a crime more burdensome after its commission, or which deprives a defendant of a defense available when the act was committed."[51] Thus, if the court holds that the outdated New Jersey identity theft statute did not apply to Thornton's actions, it would be unconstitutional for any amended statute to apply retroactively to Thornton's conduct.

Federal courts have had similar difficulties in attempting to apply ambiguous statutory language to Internet impersonation cases.[52] In one of the most tragic online impersonation cases in the last decade, a Missouri woman, Lori Drew, was prosecuted under federal law when her atrocious actions led to the suicide of Megan Meier, a thirteen-year-old classmate of Drew's daughter.[53] Drew and other co-conspirators registered a fictitious profile on the website MySpace.com ("MySpace"), impersonating a boy named Josh Evans.[54] "The conspirators contacted Megan through the MySpace network . . . using the Josh Evans pseudonym and began to flirt with her over a number of days."[55] In one of the last communications with Megan, "the conspirators had 'Josh' tell Megan that he no longer liked her and that 'the world would be a better place without her in

---

[49] *See* Edward A. Zunz, Jr. & Edwin F. Chociey, Jr., *Review of Statutes And Other Legislation*, 40 N.J. PRAC., APPELLATE PRACTICE AND PROCEDURE § 4.26 (2d ed. 2011) ("Courts can apply statutes retroactively under appropriate circumstances, but courts generally favor prospective application of statutes. Courts will use a two-part test to determine whether a statute should apply retroactively; the first inquiry is whether the legislature intended to give the statute retroactive application, and the second question is whether the statute's retroactive application will result in either an unconstitutional interference with vested rights or a manifest injustice.").

[50] U.S. CONST. art. 1 § 10, cl. 1; N.J. CONST., art. IV, § VII. par. 3 (amended 1947).

[51] State v. T.P.M., 460 A.2d 167, 170 (N.J. Super. Ct. App. Div. 1983).

[52] *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009) (stating that the meaning of the elements in the Computer Fraud and Abuse Act ("CFAA") is controversial, yet the court decided to apply it to Drew's case anyway).

[53] *Id.* at 452.

[54] *Id.*

[55] *Id.*

it.' "[56] Shortly thereafter, Megan committed suicide.[57]

State and federal officials in Missouri decided not to prosecute Drew due to the lack of applicable criminal charges that corresponded with Drew's actions.[58] The Missouri officials' acquiescence led to an array of public outrage and scrutiny.[59] In response, the Los Angeles United States Attorney's Office elected to prosecute Drew under the Computer Fraud and Abuse Act ("CFAA").[60] The CFAA makes it a misdemeanor offense when a defendant "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[61] The court in *Drew* emphasized that the central issue in the CFAA analysis was whether Drew's conscious violations of MySpace's terms of service satisfied the statutory language of the CFAA.[62] The court held that Drew's breach of the MySpace terms of services satisfied the intentional access or exceeding authorized access element of the CFAA.[63]

The court then analyzed "whether basing a CFAA misdemeanor violation . . . upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine."[64] "The void-for-vagueness doctrine has two prongs: a . . . notice sufficiency requirement, and . . . a guideline setting element to

---

[56] *Id.*

[57] *Drew*, 259 F.R.D. at 452.

[58] Amanda Harmon Cooley, *Guarding Against a Radical Redefinition of Liability for Internet Misrepresentation: The* United States v. Drew *Prosecution And the Computer Fraud And Abuse Act*, 14 J. INTERNET L. 1, 14 (2011) (citing David Hunn & Tim Bryant, *Newspaper Is Denied Access to FBI Records in Suicide Investigation*, ST. LOUIS POST-DISPATCH, Dec. 21, 2007, at C3, *available at* 2007 WLNR 25214100).

[59] *Id.*

[60] *Id.*; 18 U.S.C. § 1030 (Supp. II 2008); *see also* Jennifer Steinhauer, *Woman Found Guilty in Web Fraud Tied to Suicide*, N.Y. TIMES, Nov. 27, 2008, at A25, *available at* 2008 WLNR 22673768. "Thomas P. O'Brien, the United States attorney in Los Angeles, prosecuted the case himself with two subordinates after law enforcement officials in Missouri determined Ms. Drew had broken no local laws." *Id.* The attorneys successfully asserted jurisdiction on the ground that MySpace is based in Los Angeles, California. *Id.*

[61] 18 U.S.C. § 1030(a)(2)(C).

[62] *Drew*, 259 F.R.D. at 458 ("[T]he primary question here is whether any conscious violation of an Internet website's terms of service will cause an individual's contact with the website via computer to become 'intentionally access[ing] . . . without authorization' or 'exceeding authorization.' " (second and third alternations in original) (quoting 18 U.S.C. § 1030(a)(2) (Supp. II 2008))).

[63] *Id.* at 461.

[64] *Id.* at 464.

govern law enforcement."[65] As for the notice prong, the court articulated that the relevant question was "whether individuals of 'common intelligence' are on notice that a breach of a terms of service contract can become a crime under the CFAA."[66] The court held that these individuals would not be on notice, and therefore concluded that the first prong of the doctrine was satisfied.[67] With respect to the second prong, the court held that "[t]reating a violation of a website's terms of service . . . to be sufficient to constitute [the CFAA's intentional unauthorized access element] would result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals."[68] The court mentioned that the victim in the case, Megan, was also in clear violation of one of the MySpace terms of service provisions, which required MySpace users to be at least fourteen years old.[69] The court held that the second prong for the void-for-vagueness doctrine was satisfied and concluded:

> [I]f any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[70]

Many experts in the field of cyberlaw believe that the government's argument in *Drew* was an unwarranted expansion of what Congress intended the CFAA to include.[71] It is likely that the

---

[65] *Id.* at 463.

[66] *Id.* at 464.

[67] *Drew*, 259 F.R.D. at 464.

[68] *Id.* at 466.

[69] *Id.*

[70] *Id.* at 467 (second alteration in original) (quoting City of Chi. v. Morales, 527 U.S. 41, 64 (1999)).

[71] *See* Steinhauer, *supra* note 60 (quoting a former federal prosecutor who said, "As a result of the prosecutor's highly aggressive, if not unlawful, legal theory . . . it is now a crime to 'obtain information' from a [w]eb site in violation of its terms and service. This cannot be what Congress meant when it enacted the law, but now you have it").

Missouri officials were correct in not prosecuting Drew,[72] and some believe that the United States Attorney in Los Angeles had ulterior motives in prosecuting Drew due to the increasing media coverage of the case.[73] Unquestionably, the egregious facts in Drew's case led to her prosecution, but regardless of the motivations that gave rise to *Drew*, Drew's counsel successfully convinced the court that the CFAA does not apply to online impersonation.[74] The decision in *Drew* exemplifies the unexplainable absence of any applicable federal statute explicitly dealing with the issue of Internet impersonation.

Although Congress has not enacted a statute dealing with the issue of impersonation on the Internet, New Jersey and other states are following the lead of California and New York in criminalizing the creation of fake social networking profiles to injure innocent victims.[75] The urgency for Congress to enact an Internet impersonation statute is exemplified by the number of recent civil cases which have been filed in different states against perpetrators and social networking sites for damages resulting from creating a fake social networking profile.[76] It is fascinating to speculate what the results of some of these civil cases would be if the perpetrators were prosecuted under the applicable identity theft statute of that state.

In Texas, two high-school students created a MySpace profile impersonating their vice-principal, Anna Draker.[77] The profile, which appeared to be created by Draker, "contained her name, photo, and place of employment, [and included] explicit and graphic sexual references."[78] Draker claimed that the students created a website containing "lewd, false, and obscene comments, pictures, and

---

[72] Cooley, *supra* note 58.

[73] *See* Steinhauer, *supra* note 60 (referring to Drew's attorney, who believed that "the trial was grandstanding by Mr. Obrien [the United States Attorney on the case] in an effort to keep his job").

[74] *See Drew*, 259 F.R.D. at 464 (concluding that MySpace's "terms of service runs afoul of the void-for-vagueness doctrine").

[75] *Internet Imposters*, STATE LEGISLATURES, May 1, 2010, at 8, *available at* 2010 WLNR 10273597 (stating that Internet impersonation bills were introduced in Pennsylvania and West Virginia).

[76] Kay, *supra* note 11, at 3.

[77] Draker v. Schreiber, 271 S.W.3d 318, 320-21 (Tex. App. 2008).

[78] *Id.* at 320.

graphics that implied she was a lesbian."[79] Draker originally sued the students for "defamation and libel per se, as well as [the students'] parents for negligence and gross negligence relating to the parents' supervision of the students' use of the [I]nternet."[80] Draker amended her complaint multiple times and ultimately only a claim for intentional infliction of emotional distress reached the Texas Court of Appeals.[81] The court denied Draker any relief for her claim of intentional infliction of emotional distress and her claim was dismissed.[82]

In 2008, when *Draker* was decided, Texas had not yet passed its "online impersonation" statute.[83] At that time, the only option available for prosecutors in such a case was to use the outdated Texas identity theft statute, which stated that a person is guilty of identity theft if he or she "with intent to harm or defraud another, obtains, possesses, transfers, or uses an item of . . . [personal] identifying information of another person without the other person's consent."[84] The old Texas statute was similar to the federal identity theft statute, which was mainly concerned with protecting consumers from financial injury.[85] Under current Texas law, however, a person is guilty of online impersonation, a third degree felony, when he or she "create[s] a web page on a commercial social networking site" to harm or defraud the victim.[86] It is quite possible that the high-school students in the *Draker* case would have been aggressively prosecuted and likely held guilty under the current online impersonation statute.[87]

B. Stealing the Password of the Victim

The second way that an issue of identity theft on the Internet

---

[79] *Id.* at 324.

[80] *Id.* at 321.

[81] *Id.*

[82] *Draker*, 271 S.W.3d at 325.

[83] *See* TEX. PENAL CODE ANN. § 33.07 (West 2011).

[84] TEX. PENAL CODE ANN. § 32.51 (West 2011).

[85] 18 U.S.C. § 1028(a)(7) (2006).

[86] TEX. PENAL CODE ANN. § 33.07.

[87] *See id.* (holding a person liable if he or she "create[s] a web page on a commercial social networking site" without consent); *Draker*, 271 S.W.3d at 320-21 (showing that the students had created a fake profile without the consent of their principal).

can potentially arise is when the perpetrator steals or somehow gains access to the victim's social media account, and subsequently impersonates that victim.[88] Though the methodology of impersonating the victim is different in such a case, courts and legislatures have successfully applied identity theft statutes or state and federal cyberstalking statutes.[89] However, when the perpetrator impersonates a victim by stealing his or her password, more complications can arise: potential hackers may have the ability to steal valuable financial information or inflict fatal viruses on the victim's computer.[90]

Hacking into social media accounts has been linked to all types of relationships, with dating relationships being the most prominent.[91] Close friends or couples usually do not think twice about disclosing their passwords for Facebook or Twitter to each other, but recent stories around the country emphasize the necessary caution that must be exercised before disclosing such personal information.[92] One such case involves a twenty-five-year-old woman from Minnesota who was recently charged with "taking over [her former friend's] Facebook account to send messages such as 'fat lard,' 'you are so gross,' and 'the game's only begun.' "[93] The

---

[88] *See, e.g.*, *In re Rolando S.*, 129 Cal. Rptr. at 52.

[89] *See, e.g.*, Tom Zeller Jr., *Despite Laws, Stalkers Roam on the Internet*, N.Y. TIMES, Apr. 17, 2006, at A1, *available at* 2006 WLNR 6394945 (applying cyberstalking statutes to cases where the perpetrator gains access to the victim's profile).

[90] *See Facebook Fraud: Identity Theft Through Social Networking*, PROTECTMYID, http://www.protectmyid.com/images/education_center/pdf/050Typesof Fraud/7_types%20of%20fraud_social%20networking.pdf (last visited Nov. 27, 2012) ("Variations on many well-known email scams have quickly made their way onto networking sites. The sites work hard to identify and prevent misuse of their systems, but phishing scams, malware, and cons for cash have all occurred.").

[91] *See* Joy Powell, *Stalkers and Harassers Plunge into Social Media Beware Who Your Friends Really Are: More People Are Taking Over Accounts, Creating Fake Profiles in "A New Kind of Crime,"* STAR TRIBUNE, Jan. 15, 2011, at 01A, *available at* 2011 WLNR 1017657. The author quotes Jill Oliveira, spokeswoman at the Minnesota Bureau of Criminal Apprehension, stating: "We have had a few cases with people initiating false Facebook accounts and MySpace accounts . . . . Usually the person who starts the account is an ex-boyfriend or ex-girlfriend. They tend to have a vendetta against the individual and have access to pictures to upload to the false accounts." *Id.* (internal quotation marks omitted).

[92] *See id.* (discussing multiple cases of former friends or exes who steal passwords, including a woman from Minnesota who faces felony charges for stealing "others' Facebook and email accounts to send hateful messages").

[93] *Id.*

Minnesota woman now has a "restraining order barring her from impersonating her former friend and [her former friend's] husband on Facebook."[94] In another case, a twenty-six-year-old man from Minnesota was "recently convicted of hijacking a neighbor's e-mail to send pornographic photos to the neighbor's co-workers."[95]

Other times, victims may have no idea who hacked into their account, making it very difficult for officials to find the perpetrator and making it harder for the victim to escape this nightmare.[96] Claire E. Miller, a publishing executive in Manhattan, was one of the many victims of what has been defined as cyberstalking.[97] Cyberstalking appears in various different forms: "Installing spyware on a target's computer[;] . . . GPS (global positioning system) surveillance of the . . . victim[]; posting personal or false and humiliating information about the victim on the Internet; sending harassing emails and text message[s;] and using social media such as Facebook or Twitter to post false and humiliating information."[98] Miller had been victimized by constant and disturbing "phone calls, e-mail messages[,] and even late-night visits from strange men" who were seeking delivery on provocative promises made to them by an online impersonator.[99]

Unfortunately, Miller is not alone in this battle. Recent studies show that "[forty percent] of women have experienced dating violence via social media [sites] . . . [twenty percent] of online stalkers use social networking to stalk their victims[,] [and] [thirty-four percent] of female college students [along with fourteen percent] of male students have broken into a romantic partner's email."[100] A psychologist in private practice in Long Island, New York, Elizabeth Carll, explained that victims of cyberstalking experience many negative emotional reactions.[101] Carll stated : " 'If you're harassed in

---

[94] *Id.*

[95] Powell, *supra* note 91.

[96] Zeller, *supra* note 89 (demonstrating that in half the cases, the victim and perpetrator are complete strangers).

[97] *Id.*

[98] Charlene Laino, *'Cyberstalking': Worse Than In-Person Harassment?*, WEBMD (Aug. 8, 2011), http://www.webmd.com/balance/news/20110808/cyberstalking-worse-than-in-person-harassment.html.

[99] Zeller, *supra* note 89.

[100] Laino, *supra* note 98.

[101] *Id.* ("[V]ictims of cyberstalking have a wide range of emotional reactions, including

school or work, you can come home to a safe environment[,] . . . [but] [i]f you're cyberstalked, it can be all the time, no matter where you are.' "[102] Carll stressed that people must protect themselves from impersonation and cyberstalking by creating secure passwords and not giving their passwords to anyone.[103]

While some perpetrators hack into a victim's social media account for the purpose of stalking or tormenting the victim, other perpetrators steal the passwords of innocent users for the purpose of obtaining valuable financial information.[104] Many well-known email scams that have existed for years are migrating their way into social networking sites.[105] One example is a scam on Twitter in which messages are sent to Twitter members impersonating one of the members' friends.[106] These messages are actually sent by trained hackers and carry links "designed to steal passwords and recruit people for work-at-home schemes to [labor] as money mules," so that the hackers can set up "bank accounts to help thieves extract [finances] from hijacked financial accounts."[107] In early 2012, Facebook had trouble with a developing scam in which hackers hijacked accounts and then impersonated Facebook security.[108] The impersonated security team sent a personal message to friends, reading: "Last Warning: Your Facebook account will be turned off because someone has reported you. Please do re-confirm your account security by: (link)."[109] The link in the message then sent the potential victim to a fake page that looked like Facebook, but was actually an external domain; once there, users were told to enter their personal information and credit card information.[110]

Another similar scam arises when a thief steals a person's

---

high levels of stress, anxiety, fear, and helplessness as well as nightmares, hypervigilance, undereating or overeating, and sleeping difficulties.").

[102] *Id.*

[103] *Id.*

[104] *Facebook Fraud*, *supra* note 90, at 1.

[105] *Id.*

[106] Byron Acohido, *Scammers Hit Twitter with Tainted Tweet Storm Cybervillains Repurpose E-mail Spam Techniques*, USA TODAY, Sept. 29, 2009, at 7A, *available at* 2009 WLNR 19162424.

[107] *Id.*

[108] *Hackers Impersonate Security Team on Facebook*, FACECROOKS (Jan. 17, 2012), http://facecrooks.com/Scam-Watch/hackers-impersonate-security-team-on-facebook.html.

[109] *Id.*

[110] *Id.*

online identity and subsequently sends a desperate plea, in a message format, for cash to the member's online friends.[111] A typical message may state, "I'm traveling abroad and all of my money and documents have been lost. Please wire me $500 so I can get home."[112] Naïve, but concerned, family members and friends may be tricked by the hacker and send the money.[113] Hackers can obtain passwords through phishing scams or malware, and by simply downloading an application or taking an online quiz; thus, innocent victims can be providing hackers with the ability to track future activities for the purpose of accessing the victims' identification names and passwords for financial accounts.[114]

Appropriate officials may have trouble ascertaining the identities of hackers who steal passwords through social networking sites; however, if the identities are discovered, federal and state cyberlaws exist to deal with these issues.[115] In the federal context, as long as there is an economic detriment to the victim, the CFAA can be utilized to prosecute impersonating hackers.[116] On the state level, most states have identity theft statutes explicitly prohibiting online impersonation to obtain financial records.[117]

Unlike the difficulties of prosecuting impersonators who create completely fake profiles, there is substantially less difficulty in prosecuting online imposters for the act of stealing passwords or personal information, which is interpreted as a medium to "cyber-stalk" victims.[118] California and forty-five other states have enacted anti-cyberstalking laws within the last decade; on the federal level, women can also seek protection under the "Violence Against Women and Department of Justice Reauthorization Act of 2005,"[119] which

---

[111] *Facebook Fraud*, *supra* note 90, at 1.

[112] *Id.*

[113] *Id.*

[114] *Id.* at 1-2.

[115] Zeller, *supra* note 89.

[116] 18 U.S.C. § 1030(g) (2006).

[117] *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-2008(A) (2004) (West); N.Y. PENAL LAW § 190.25(1) (McKinney 2008); CAL. PENAL CODE § 530.5(a) (West 2011).

[118] *See* Zeller, *supra* note 89 (demonstrating how a former security guard was sentenced to six years in prison under the California cyberstalking law for using his ex-girlfriend's personal information to impersonate her in chat rooms and personals sites. While impersonating his girlfriend, "[h]e posted rape fantasies . . . [and] begged strangers to deliver on them" after giving strangers his ex-girlfriend's home address).

[119] Violence Against Women and Department of Justice Reauthorization Act of 2005,

"updated telephone harassment law to include computer communications."[120]

An issue that now presents itself is, what type of Internet impersonation would not be considered cyberstalking and therefore not be prosecutable under the cyberstalking statutes.[121] The determinative factor on whether a perpetrator will be prosecuted under an identity theft statute or a cyberstalking statute seems to be the foreseeable harm from the perpetrator's impersonation.[122] In *In re Rolando S.*, a teenager was prosecuted under the California identity theft statute, not the cyberstalking statute, when he gained access to a classmate's Facebook page and posted explicit sexual material on it.[123] On the other hand, a California man, Gary S. Dellapenta, who impersonated his ex-girlfriend by stealing her personal information to access a dating website, causing multiple men to arrive at her house, was prosecuted under the California cyberstalking statute.[124] The foreseeable harm for the victim in *In re Rolando S.* was sufficiently less than the foreseeable harm to Dellapenta's ex-girlfriend because the latter was subjected to the arrival of strange men at her doorstep.

Thus, it seems that cyberstalking statutes are often triggered when the victim is more likely to be placed in reasonable fear of his

---

Pub. L. No. 109-162, 119 Stat. 2960 (2006).

[120] Zeller, *supra* note 89.

[121] *See* CAL. PENAL CODE § 653.2(a) (West 2010). Section 653.2(a) states:

> Every person who, with intent to place another person in reasonable fear for his or her safety, or the safety of the other person's immediate family, by means of an electronic communication device, and without consent of the other person, and for the purpose of imminently causing that other person unwanted physical contact, injury, or harassment, by a third party, electronically distributes, publishes, e-mails, hyperlinks, or makes available for downloading, personal identifying information, including, but not limited to, a digital image of another person, or an electronic message of a harassing nature about another person, which would be likely to incite or produce that unlawful action, is guilty of a misdemeanor punishable by up to one year in a county jail, by a fine of not more than one thousand dollars ($1,000), or by both that fine and imprisonment. *Id.*

[122] *Compare In re Rolando S.*, 129 Cal. Rptr. 3d at 51-52 (electing to prosecute defendant under an identity theft statute because the posting of embarrassing comments was not very dangerous), *with* Zeller, *supra* note 89 (sentencing ex-boyfriend who posted rape fantasies under his ex-girlfriend's name under the cyberstalking statute).

[123] *In re Rolando S.*, 129 Cal. Rptr. 3d at 51-52.

[124] Zeller, *supra* note 89; *see* CAL. PENAL CODE § 653.2.

or her safety.[125] However, prosecutors are more likely to utilize identity theft statutes when the online impersonation caused some sort of harm to the victim, but the victim was not placed in reasonable fear of his or her safety.[126] Thus, the controlling factor to determine what statutory scheme should be used is the degree of harm the victim confronts.[127]

III. APPLICABLE STATUTES CONCERNING IDENTITY THEFT ON THE INTERNET

A. Original Identity Theft Statutes

The earliest identity theft statute in the United States was enacted in 1996 in Arizona.[128] The Arizona statute renders a perpetrator guilty of identity theft when he or she:

> [K]nowingly takes . . . or uses any personal identifying information . . . of another person[,] . . . including a real or fictitious person or entity, without the consent of that other person or entity, with the intent to obtain or use the other person's or entity's identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense . . . .[129]

The Arizona legislature sought to deter potential perpetrators by stressing the severity of the offense and labeling the crime of identity theft as a class 4 felony.[130] In Arizona, a class 4 felony "translates into a sentence of between one-and-one-half and three years in prison

---

[125] *See In re Rolando S.*, 129 Cal. Rptr. 3d at 51-52 (prosecuting defendant under the California identity theft statute and not the cyberstalking statute).

[126] *See, e.g.*, Zeller, *supra* note 89 (sentencing ex-boyfriend who posted rape fantasies under his ex-girlfriend's name under the cyberstalking statute).

[127] *Compare* Zeller, *supra* note 89 (prosecuting under cyber stalking statute because conduct created a risk of reasonable harm), *with In re Rolando S.*, 129 Cal. Rptr. 3d at 51-52 (applying identity theft statute when victim's Facebook page was used by defendant to post obscene material because no great risk of harm was generated).

[128] Catherine Pastrikos, Comment, *Identity Theft Statutes: Which Will Protect Americans the Most*, 67 ALB. L. REV. 1137, 1138 (2004); *see also* ARIZ. REV. STAT. ANN. § 13-2008 (2004) (West).

[129] ARIZ. REV. STAT. ANN. § 13-2008.

[130] *Id.* at § 13-2008(F); *see also* Pastrikos, *supra* note 128.

for first time offenders."[131] Even today, Arizona's statute is silent on the issue of identity theft on the Internet.[132] However, as with laws in other jurisdictions, the excessively broad language in the Arizona statute would probably force many Arizona judges to determine that knowingly taking or using another person's social media account "without the consent of that other person" and "with the intent to obtain or use the other person's" social media account to "cause loss" to the other person[133] would satisfy the identity theft statute.[134]

In 1998, two years after Arizona's state statute was implemented, Congress enacted the Federal Identity Theft and Assumption Deterrence Act.[135] The Act made it a federal crime to knowingly possess or use, "without lawful authority, a means of identification of another person with the intent to commit . . . any unlawful activity that constitutes a violation of Federal law, or . . . any applicable State or local law . . . ."[136] The Act addressed identity theft on the federal level in two ways: it "strengthen[ed] the criminal laws governing identity theft," and it focused on the consumers as the victims.[137] The federal law on identity theft is specifically directed at economic losses suffered by consumers.[138] This is in direct contrast to the Arizona statute, which explicitly states that economic loss to the victim is not required.[139] Thus, under the federal statute, or any statute similar, the prosecution of a perpetrator of identity theft on a social media site for non-economic purposes would likely be dismissed.[140]

---

131 Pastrikos, *supra* note 128; *see also* ARIZ. REV. STAT. ANN. § 13-702(D) (2004) (West).

132 *See* ARIZ. REV. STAT. ANN. § 13-2008.

133 *Id.*

134 *See* Hansen, *supra* note 1 (paraphrasing a judge who held that the prosecution of a woman for impersonating her ex-boyfriend by creating a fake Facebook account would proceed, even though the New Jersey statute was silent concerning electronic communications, specifically Internet communications).

135 18 U.S.C. § 1028(a)(7) (2006); Pastrikos, *supra* note 128, at 139-40; *see also* Charles Harwood, Dir., *Identity Theft* (Jan. 29, 2001), *available at* 2001 WL 85693, at *1.

136 18 U.S.C. § 1028(a)(7).

137 Harwood, *supra* note 135.

138 *See* S. REP. NO. 105-274, at 4 (1998) (listing that the second purpose of the bill is "to recognize the individual victims of identity theft crimes, and establish their right to restitution to include all costs related to regaining good credit or reputation.").

139 ARIZ. REV. STAT. ANN. § 13-2008(A) (2004) (West).

140 *Compare* 18 U.S.C. § 1028(a)(7) (requiring a financial detriment as a key element to the statute), *with* N.C. GEN. STAT. ANN. § 14-113.20(a) (West 2005) (requiring a financial detriment as a key element to the statutory provision).

B. New York Identity Theft Statute

Under New York law, "A person is guilty of criminal impersonation in the second degree when he . . . [i]mpersonates another by communication by [I]nternet website . . . with intent to obtain a benefit or injure or defraud another . . . ."[141] New York was the first state to implement such explicit language concerning identity theft on the Internet into a separate subdivision of its identity theft statute.[142] On March 23, 2007, the New York Senate and Assembly unanimously approved the memorandum in support of the legislative bill, which amended the identity theft statute to incorporate Internet impersonation.[143] The memorandum stressed that Internet "impersonation has become an increasingly large problem in the United States" because of the ease of impersonating another via Internet communications.[144] It further directed that "misrepresenting oneself through the use of the Internet become a crime in order to deter the plethora of cases presently occurring."[145]

The memorandum also mentioned an incident of Internet impersonation in Suffolk County that prompted the Senate to take action.[146] In this incident, Michael Valentine, a Suffolk County police officer, "hack[ed] into the Yahoo e-mail account of a woman he had briefly dated and posing as her [during] online communications."[147] The Suffolk County District Attorney discovered that Mr. Valentine "accessed the woman's personal profile on the dating site Match.com, sending electronic 'winks' and other [electronic] communications to 70 different men on the site."[148] Two men even showed up to the woman's house after communicating with Valentine through her Match.com profile.[149]

The memorandum emphasized countless numbers of documented cases like Valentine's, "where perpetrators gain access into another person['s] account and pose as them through the use of

---

141 N.Y. PENAL LAW § 190.25(4) (McKinney 2008).
142 *See id.*
143 S. 4053, 2007-2008 Reg. Sess. (N.Y. 2008).
144 *Id.*
145 *Id.*
146 *Id.*
147 Zeller, *supra* note 89.
148 *Id*.
149 *Id*.

online communications."[150] The New York legislature's findings were indeed accurate, with similar Internet impersonation horror stories appearing all over the country.[151] The New York legislature has been a pioneer in the effort to protect victims of Internet identity theft, as is evidenced by the new identity theft statute.[152] Other jurisdictions would be wise to follow the footsteps of the New York Senate by creating an explicit subdivision dealing with Internet impersonation within their respective identity theft statutes, thus eliminating the potential ambiguity an identity theft statute may have concerning internet impersonation.

C. California Identity Theft Statute

California took an even a bigger step than New York when it enacted its Internet identity theft statute in January 2011.[153] Rather than just adding a separate subdivision on Internet impersonation like New York, California created a completely separate statute in order to protect its citizens from Internet identity theft.[154] The statute states that "any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site . . . for purposes of harming, intimidating, threatening, or defrauding another person is guilty" of identity theft.[155]

Unlike previous statutes, section 528.5 made specific purposes such as "harming, intimidating, threatening, or defrauding" illegal after the perpetrator has gained access to the victim's profile.[156] The California legislature's implementation of these specific purposes reached the heart of the most devastating effects of Internet impersonation. Traditionally, "harming, intimidating, threatening, or defrauding"[157] a person by impersonation on the

---

[150] N.Y. S. 4053.

[151] *See, e.g.*, Hansen, *supra* note 1 ("Bradley Shear, a Bethesda, Md., lawyer who specializes in online issues, said he expects to see more cases like this one in the near future."); *Drew*, 259 F.R.D. 449.

[152] Hansen, *supra* note 1.

[153] *See* CAL. PENAL CODE § 528.5 (West 2011).

[154] *Id.*

[155] *Id.*

[156] *Id*.

[157] *Id.*

Internet has only given rise to civil, but not criminal, liability.[158] However, California retreated from this traditional notion by criminalizing Internet impersonation.[159]

In response to the vague reasoning the California Court of Appeals provided in *In re Rolando S.*, the California legislature enacted section 528.5.[160] The lengthy and ambiguous analysis concerning the legislature's intent on what qualifies as an unlawful purpose in *In re Rolando S.* was clarified by the enactment of section 528.5; California's current Internet impersonation statute is one of the most sophisticated statutes concerning Internet identity theft.[161] In a world where young people naively divulge too much information on social networking sites, sophisticated and explicit statutes dealing with Internet impersonation are absolutely necessary. Experts believe that Internet impersonation cases are on the rise,[162] but it seems that only a few states are taking the appropriate legislative steps to deter potential perpetrators.[163]

D. Other States' Statutory Schemes Corresponding with Online Impersonation

In late 2011, Texas enacted an "online impersonation" statute, which makes it a third degree felony when a perpetrator "without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to . . . create a web page on a commercial social networking site or other Internet website; or . . . post . . . messages on or through a commercial social networking site."[164] The Texas

---

[158] Kay, *supra* note 11, at 17.

[159] *See In re Rolando S.*, 129 Cal. Rptr. 3d at 58 (finding appellant's conduct to be a criminal offense).

[160] *See id.* at 55-56 ("[T]he Senate Committee report for the bill introducing the amendment makes clear that the purpose of the 'any unlawful purpose' language was to broaden the scope of punishable conduct."); CAL. PENAL. CODE § 528.5.

[161] *See* CAL. PENAL. CODE § 528.5.

[162] Hansen, *supra* note 1.

[163] *See Internet Imposters*, *supra* note 75 (showing that California, New York, Pennsylvania, and West Virginia were the few states to introduce Internet impersonation bills).

[164] TEX. PENAL CODE ANN. § 33.07 (a)(1)(2) (West 2011).

statute contains effective statutory language to criminalize both methods of online impersonation.[165] Provision (a)(1) explicitly prohibits a person from "creat[ing] a web page on a commercial social networking site," and unambiguously criminalizes any person who creates a fake profile impersonating another person with the purpose to "harm, defraud, intimidate, or threaten" that person.[166] Under (a)(2) of the statute, a person is guilty if he or she "post[s] . . . one or more messages . . . through a commercial social networking site" while using the name of another person.[167] This subdivision implicitly applies to the stealing method of Internet impersonation and a Texas perpetrator will undoubtedly be found guilty under the statute if he or she gains access to a victim's account by stealing personal information and subsequently purports to be that person by sending lewd messages within the victim's social network.[168]

Unlike Texas, some states would have an immense amount of difficulty in attempting to prosecute a perpetrator for either of the two methods of online impersonation. For example, North Carolina has an identity theft statute that makes it illegal for a person to use another's identifying information "for the purposes of making financial or credit transactions."[169] North Carolina also has a cyber-bullying statute that makes it illegal to "[b]uild a fake profile or [w]eb site" if "the intent [was] to intimidate or torment a minor."[170] Thus, the North Carolina legislature is only concerned with Internet identity theft in the financial context and in protecting minors.[171] As many cases around the nation point out, however, online impersonation on social media sites can cause serious issues outside the financial realm and affect victims of all ages.[172]

---

[165] *See id.* (covering cases where an impersonator either creates the web page, or posts messages on the victim's already existing web page, without the victim's consent).

[166] *Id.*

[167] *Id.* at § 33.07 (a)(2).

[168] *See id.* (criminalizing Internet impersonation).

[169] N.C. GEN. STAT. ANN. § 14-113.20(a) (West 2005).

[170] N.C. GEN. STAT. ANN. § 14-458.1(a)(1)(a) (West 2009).

[171] *See id.*; N.C. GEN. STAT. ANN. § 14-113.20.

[172] Zeller, *supra* note 89 (discussing multiple cases of women over the age of eighteen who suffered serious consequences from a perpetrator who impersonated their identities online).

IV. IDEAL STATUTE AND OTHER SOLUTIONS TO PREVENT THE HARMS OF IDENTITY THEFT ON THE INTERNET

A. Ideal Statute

As this Comment has explained, identity theft on the Internet is a real and serious issue in our society.[173] States that do not implement sophisticated statutes which explicitly incorporate different methods of online impersonation are subjecting their citizens to potentially disastrous consequences.[174] Outdated identity theft statutes that are mainly concerned with financial detriments are not sufficient to encompass online impersonation within their statutory framework.[175] On the other hand, states that enacted a statute or subdivision to prevent online impersonation are at the forefront of protecting the psychological and emotional well being of potential victims.[176]

Unfortunately, "[t]he Internet knows no jurisdictional boundaries," and states such as California and New York may have trouble in enforcing online impersonation statutes if the perpetrator lives outside of the state.[177] There is no question that every state should make an effort to produce some type of legislation dealing with online impersonation; however, the only way to successfully punish and deter online impersonation is for Congress to enact a federal statute that explicitly recognizes and prohibits online impersonation through social networking media sites.[178] An ideal federal statute should be based on the current New York and California statutes, which acknowledge the two different methods for online impersonation within the statutory language and recognize specific types of websites that are susceptible to online

---

[173] *See supra* Part II. A-B.

[174] *See Drew*, 259 F.R.D. at 452 (showing that a thirteen-year-old-girl committed suicide after her classmate's mother impersonated a young boy to ridicule her).

[175] *See id.* at 464 (holding that the CFAA did not encompass online impersonation); *see also* 18 U.S.C. § 1028(a)(7) (2006); *Draker*, 271 S.W.3d at 325 (holding that two teens impersonating their principal were not even subject to civil liability).

[176] *See* N.Y. PENAL LAW § 190.25(4) (McKinney 2008); *see also* CAL. PENAL CODE § 528.5 (West 2011).

[177] Hansen, *supra* note 1 (internal quotation marks omitted) (quoting Bradley Shear, Esq.).

[178] *See* 18 U.S.C. § 1028(a)(7) (indicating that the current federal identity theft statute does not adequately recognize online impersonation); 18 U.S.C. § 1030 (2006) (showing how the CFAA similarly does not adequately recognize online impersonation).

impersonation.[179]

The New York and the California statutes use similar statutory language to identify the potential actions that give rise to online impersonation.[180] The New York statute holds a perpetrator guilty of criminal impersonation if he or she "[i]mpersonates another by communication by [I]nternet website or electronic means."[181] Similarly, the California statute holds a person guilty of impersonation when he or she "credibly impersonates another actual person through or on an Internet [w]eb site or by other electronic means."[182] These statutes are unnecessarily broad because online impersonation, with respect to social media sites, can occur in only two ways: either by stealing personal information to gain access or by creating a fake profile.[183] Thus, an ideal statute should explicitly state that a person would be guilty of criminal impersonation if he or she impersonates another person by creating a fake profile of another person or by wrongfully gaining access to the victim's account. In order to stay on the safe side a term such as "or [by other] electronic means," which is evident in the New York and California statutes, should follow the two methods.[184]

The next phrase that is required within the statutory framework is to identify what type of conduct and injury will be punishable when an impersonation occurs.[185] The New York online impersonation statute requires the potential perpetrator to act "with [the] intent to obtain a benefit or injure or defraud another,"[186] while the California statute also includes "harming, intimidating, [and] threatening" the victim as punishable conduct.[187] In many situations, it may be difficult to ascertain whether a perpetrator's actions actually "injure or defraud" the victim, but the victim nevertheless experiences severe psychological or emotional harm.[188] This is

---

[179] *See* N.Y. PENAL LAW § 190.25(4); CAL. PENAL CODE § 528.5.

[180] *See* N.Y. PENAL LAW § 190.25(4); CAL. PENAL CODE § 528.5.

[181] N.Y. PENAL LAW § 190.25(4).

[182] CAL. PENAL CODE § 528.5.

[183] *Facebook Fraud*, *supra* note 90.

[184] N.Y. PENAL LAW § 190.25(4); CAL. PENAL CODE § 528.5.

[185] *See* Horowitz, *supra* note 21 (discussing a dispute over whether there was sufficient injury under the applicable statute).

[186] N.Y. PENAL LAW § 190.25(4).

[187] CAL. PENAL CODE § 528.5.

[188] *See Drew*, 259 F.R.D. at 452 (explaining how a thirteen-year-old girl committed

precisely why an ideal statute would mimic the types of conduct listed in the California statute.[189] The four types of conduct listed in the California statute protect potential victims from a wide array of foreseeable danger, while simultaneously not transforming an innocuous act of online impersonation into a crime.[190]

Finally, it is imperative for an ideal statute to include examples of the types of websites that are susceptible to online impersonation; however, this list would not be exclusive or exhaustive, and would only provide examples.[191] Though social media sites are the hotbed for online impersonation, other Internet websites such as dating websites, email websites, and other interactive sites can all lead to online impersonation and give rise to all types of negative consequences for victims.[192] In fact, some of the most dangerous online impersonation cases arise from dating websites when the perpetrator convinces random people to come to the victim's house.[193] Other horror stories include victims who are terrorized for months because the perpetrator gained access to the victim's email account and subsequently stole personal information to harm the victim.[194] The New York statute does not explicitly recognize these types of examples,[195] whereas the California statute states that " 'electronic means' shall include opening an e-mail account or an account or profile on a social networking Internet [w]eb site."[196] An ideal statute would define Internet websites and explicitly state that Internet websites would include, and not be limited to, social networking sites, email websites, dating websites, and other Internet websites requiring personal information to gain access.

---

suicide after her classmate's mom impersonated a young boy with the purpose to ridicule her); Zeller, *supra* note 89 (giving examples of two men who gave their ex-girlfriends' personal information to random men through the ex-girlfriends' dating profiles).

189 *See generally* CAL. PENAL CODE § 528.5.

190 *Id.*

191 *See* Zeller, *supra* note 89 (demonstrating that online impersonation can occur on dating websites, email websites, and online personals, in addition to social media sites).

192 *Id.*

193 *Id.*

194 *Id.*

195 *See* N.Y. PENAL LAW § 190.25(4) (McKinney 2008).

196 CAL. PENAL CODE § 528.5(c) (West 2011).

B. Collective Effort from Society to Prevent Online Impersonation

The trend to outlaw online impersonation is growing quite rapidly, yet a substantial majority of states do not have online impersonation statutes.[197] This means that there are a plethora of victims, especially children and teenagers, in the United States who are subject to being impersonated with no statutory protection available. This is precisely why people must protect themselves and their children through simple, but very effective, proactive steps to secure their social media networking accounts.[198]

Many sites, such as Facebook and Twitter, have "remember password" functions that allow users to enter the websites account without manually entering their password.[199] Social media site users should avoid these types of automatic login features and manually login in every time they enter their social media account to protect themselves from impersonation.[200] Social media site users should also be aware of the dangers present when not logging off properly from their accounts.[201] Because logging out properly after every session will protect users from online impersonation, parents or caregivers would be wise to relay this message to children who frequently are the most likely to avoid these safety precautions.[202]

Another simple but very efficient method to protect oneself from impersonation is to use strong passwords.[203] Experts recommend using passwords that contain a combination of upper and

---

[197] *See* Hansen, *supra* note 1.

[198] *See* Rob Frappier, *Protecting Your Teen from Online Impersonation*, IKEEPSAFE (July 25, 2011), http://www.ikeepsafe.org/cyberbullying-2/protecting-your-teen-from-online-impersonation/ (listing the steps that parents can take in order to protect their children).

[199] *Id.*

[200] *Id.*

[201] Linda McCarthy, Keith Watson & Denise Weldon-Siviy, *A Guide to Facebook Security: For Young Adults, Parents, and Educators*, FACEBOOK, *available at* http://www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf (last visited Jan. 8, 2013).

[202] *See id.* ("Logging out of Facebook when you're not using it is a simple and effective way to protect your account. Many people think that if they close the web page or exit the browser that also logs them out of Facebook. It doesn't."); Frappier, *supra* note 198 ("In addition to telling your kids to skip the remember password function, you should remind them to always log off after a social media session.").

[203] *Impersonation and Fraudulent Use*, UNIV. OF TORONTO, http://www.enough.utoronto.ca/computeruse/frauduse.htm (last visited Jan. 8, 2013).

lower-case letters, numbers, and symbols.[204] Strong passwords should not consist of "common words in the dictionary, or obvious things" such as one's birthday.[205] Further, users are advised to take further precaution and protect these passwords by not writing them down and not posting them or storing them on their computers.[206]

Recently, Facebook has taken its own measures to prevent online impersonation on its website.[207] Facebook created the "REPORT/BLOCK THIS PERSON" feature, which is available on the bottom-left side of every Facebook profile.[208] This feature enables users to report imposters who are impersonating victims and authorizes the Facebook security team to catch the perpetrators.[209] However, some of the reports that the Facebook security team receives are fraudulent, and thus another way in which some perpetrators harass victims.[210] In order to circumvent this problem, Facebook security requires that the complainant give a valid phone number.[211] The security team then sends a verification code to that phone number, and once the complainant enters the code into the report, the security team begins its investigation.[212] Facebook users can also use the report/block feature to report "businesses pretending to be people, and [even] hate groups masquerading as people."[213] These types of reports do not require any additional steps beyond clicking on the hyperlink on the bottom-left side of the webpage.[214]

Twitter, which is best known for the ability to interact with celebrities, has created its own method to battle online impersonation.[215] Twitter uses a "Verified Accounts" function that

---

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] *See* McCarthy et al., *supra* note 201 (teaching Facebook users how to report impersonators).

[208] *Id*.

[209] *Id*.

[210] *Id*.

[211] *Id*.

[212] McCarthy et al., *supra* note 201.

[213] *Id.*

[214] *Id.*

[215] *See* Susan M. Brazas, *Twitter Verified Accounts and Protecting Identities*, LAWYERS.COM, http://communications-media.lawyers.com/privacy-law/Twitter-Verified-Accounts-and-Protecting-Identities.html (last visited Jan. 8, 2013) ("Twitter has announced that it is launching 'Verified Accounts' in an effort to protect the integrity of its account

proves the integrity of the profile.[216] When a public official, agency, or other well-known profile is stamped with the "Verified Account" approval, then that profile is indeed what it purports be.[217]

Social media sites such as Facebook and Twitter have made valiant efforts to protect users from online impersonation. However, the only way individuals can truly protect themselves is to be aware of online impersonation and be proactive in limiting their exposure to potential risks. Social media users would be wise to keep personal information, such as their passwords, absolutely private and not hesitate to report or seek help from an external source when they fear their identity may have been impersonated.

V. CONCLUSION

Social networking sites are here to stay and it is the responsibility of the federal government and every state to protect individuals from perpetrators who seek to impersonate potential innocent victims through the use of such sites. Whether the method is by creating a fake profile or stealing personal information to access the victim's profile, Internet impersonation can be severely detrimental to potential victims. The weakest people in our society are those who decide to anonymously bash others on the Internet. These people deserve to be at least mildly punished and deterred from engaging in this conduct in the future. Unfortunately, only a handful of states have implemented statutes or subdivisions that explicitly concern identity theft on the Internet, or more specifically, online impersonation.[218] Some states possess outdated identity theft statutes that need to be modified in order to prevent difficulties when dealing with online impersonation.[219] As our world becomes more dependent on the Internet, so must our laws.

---

holders' identities.").

[216] *Id.*

[217] *Id.*

[218] *See, e.g.*, N.Y. PENAL LAW § 190.25(4) (McKinney 2008); CAL. PENAL CODE § 528.5 (West 2011); TEX. PENAL CODE ANN. § 33.07 (West 2011).

[219] *See* 18 U.S.C. § 1028(a)(7); *see also Drew*, 259 F.R.D. at 464 (holding that the CFAA did not encompass online impersonation); *Draker*, 271 S.W.3d at 325 (holding that two teens impersonating their principal were not subject to civil liability).