WE ARE NOT WHO WE PRETEND TO BE: ODR ALTERNATIVES TO ONLINE IMPERSONATION STATUTES

*Kori Clanton**

INTRODUCTION

The popularity of MTV's reality television series *Catfish*[1] and the media frenzy surrounding the death of Notre Dame football star Monti Te'O's fake online girlfriend[2] have brought the phenomenon of online impersonation to the forefront of public consciousness. A perpetrator of online impersonation is popularly referred to as a "catfish"—someone who creates a fake online persona and uses it to lure the victim into an Internet romance"[3] or otherwise deceive others. The term originates from the 2010 documentary "Catfish" in which "[y]oung filmmakers document [the now-famous, Nev Schulman's] budding online friendship with a young woman [named Megan] and her family."[4] Angela, the imposter, created the fraudulent persona of Megan using real online photographs of model, Aimee Gonzalez.[5] As one movie critic once said, "Everyone *should* see 'Catfish' "—not because of the twist, but because of how powerfully and weirdly it speaks to our time, to Internet culture and the way it allows [for] the controlled illusion of intimacy."[6] Beyond its critical representation of the falsity of many online relationships, the documentary speaks to the very real and easily accessible reality of online impersonation. As victim Aimee

* Notes Editor, *Cardozo Journal of Conflict Resolution*, Vol. 16; B.A., 2010, The George Washington University; J.D. Candidate, 2015 Benjamin N. Cardozo School of Law. The author would like to thank her family and friends for their continued support and encouragement.

1 Bryce J. Renninger, *"Catfish: The TV Show" Is Making a Name for Itself, But Is Its Premise Unraveling?*, INDIEWIRE (Jan. 18, 2013, 1:24 PM), http://www.indiewire.com/article/catfish-the-tv-show-is-making-a-name-for-itself-but-its-premise-is-unraveling?page=2#articleHeader Panel.

2 *Id*.

3 Debra Cassens Weiss, *Why Internet Imposters are Difficult to Prosecute*, (Jan. 18, 2013, 7:46 AM), *available at* http://www.abajournal.com/news/article/why_catfishing_is_difficult_to_prosecute.

4 *Catfish*, IMDB, http://www.imdb.com/title/tt1584016/ (last visited Feb. 4, 2014).

5 Gina Piccalo, *Catfish's Photo Fraud Victim*, THE DAILY BEAST (Nov. 10, 2010), http://www.thedailybeast.com/articles/2010/10/04/catfish-aimee-gonzales-speaks-out.html.

6 Alison Willmore, *"Catfish" and the Case for (Select) Spoilers*, IFC (Sept. 20, 2010, 4:09 PM), http://www.ifc.com/fix/2010/09/catfish-revisited.

Gonzalez described, "[I]t's almost worse than stealing someone's name. She actually stole my face. There's nothing more than your face that makes you who you are."[7]

In a recent *Time Magazine* article concerning the Te'O controversy, journalist Victor Luckerson appropriately asked, "Just what kind of crime is posing as someone else online, if it's a crime at all?"[8] Many social media users would be surprised to know that in fact, state legislatures are becoming increasingly concerned with how to prevent and resolve cases of online impersonation that subject its victims to humiliation, intimidation, and a host of other potentially criminal conduct resulting from the illegitimate use of one's identity online. In response, a total of nine jurisdictions have already enacted legislation against such online conduct and more are slated to follow.[9]

This Note focuses on how online dispute resolution ("ODR") processes, as opposed to litigation, offer a more efficient and effective legal solution to resolving online impersonation disputes. The purpose of this Note is to analyze the measures state legislatures and social media websites have implemented to combat online impersonation cases, and to propose a practical ODR solution that will eliminate the burdens of litigation and provide a cost-efficient and time-effective remedy. Section I provides an introduction to the current relevance and rising incidents of online impersonation via social media websites such as Facebook and Twitter. Section II explores the historical and legal contexts that have shaped the legal framework leading to the development of online impersonation legislation. Section III analyzes the effectiveness of current online impersonation statutes as applied in recent cases in leading jurisdictions to reveal inefficiencies in the litigation process. Finally, Section IV proposes the use of ODR processes and determines which methods are best adapted to resolve cases of online impersonation.

---

[7] *Id*.

[8] Victor Luckerson, *Can You Go to Jail for Impersonating Someone Online?*, TIME MAGAZINE (Jan. 22, 2013), *available at* http://business.time.com/2013/01/22/can-you-go-to-jail-for-impersonating-someone-online/.

[9] *Id*.

I. The Pervasive Issue of Online Impersonation

A. *Social Media Networking on the Rise*

Today, social networking is a major activity for Internet users among a wide range of demographic groups. Younger adults, ages eighteen to twenty-nine, are more frequent adopters but social networking continues to grow in popularity for older adults as well. According to an August 2013 Pew Research Center study, "six out of ten Internet users ages fifty to sixty-four are social networking site users, as are 43% of those ages sixty-five and older.[10] As of May 2013, almost three-quarters, 72%, of online U.S. adults used social networking sites, up from 67% in late 2012.[11] As of March 2013, Facebook reported 1.11 billion monthly active users (MAUs), up 23% from 901 million MAUs in March 2012.[12] Similarly, as of March 2013, Facebook totaled 665 million daily active users (DAUs), up from 526 million (DAUs) in March 2013.[13] Twitter, another leading social media platform that launched in 2006, currently has 218.3 million registered accounts worldwide.[14]

Facebook's 2013 U.S. Securities and Exchange Commission filing[15] disclosed that approximately eighty-three million of its user accounts were fakes or duplicates and that nearly fourteen million of those accounts were "undesirable"—created specifically by spammers or impostors to violate Facebook's terms of service.[16] Legal experts draw a distinction between "fake" and "imposter" Facebook profiles, describing fake profiles as those, which merely

---

10 Joanna Brenner and Aaron Smith, *72% of All Adults are Social Networking Site Users*, Pew Research Center (Aug. 5, 2013), http://www.pewinternet.org/~/media/Files/Reports/2013/PIP_Social_networking_sites_update.pdf.

11 *Id*.

12 Josh Constine, *Facebook's Growth Since IPO in 12 Big Numbers*, TechCruch (May 17, 2013), http://techcrunch.com/2013/05/17/facebook-growth/.

13 *Id*.

14 Josh Constine, *How Many of Twitter's 218 Million Users are Just Blind-Tweeting From Other Apps?*, TechCruch (Oct. 3, 2013), http://techcrunch.com/2013/10/03/blindtweeting/; *see also* Lucian Parfeni, *Twitter Will Continue to Grow Faster than Facebook Through 2014*, Softpedia (Mar. 6, 2013, 7:01 PM), http://news.softpedia.com/news/Twitter-Will-Continue-to-Grow-Faster-than-Facebook-Through-2014-257043.shtml.

15 U.S. Sec. and Ex. Comm'n, *Form 10Q Filings for Facebook, Inc. Quarterly Period ended June 30, 2012, available at* http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm.

16 Owen J. Sloane & Rachel M. Stilwell, *Online Impersonation*, Gladstone Michel Weisberg Willner & Sloane, ALC, (2012) http://www.gladstonemichel.com/onlineimpersonation.shtml (last visited Oct. 11, 2013).

appear real but describe someone who does not actually exist, whereas imposter profiles as those which impersonate a real-life victim whose name or likeness is being misappropriated without their consent.[17] While online impersonation statutes and legal authorities on this area of the law often use the terms fake and imposter interchangeably, it is clear that these statutes only apply to protect the likeness of a living individual, and are not intended to apply to cases of mere imaginary personas.

Given the widespread and growing adoption of social media, an individual's online persona is often the first impression that friends, potential romantic partners, and employers have of them, and it is critically important for social media users to take steps to protect their online reputation. According to a June 2013 CareerBuilder study, 43% of hiring managers who research job candidates via social media said they have discovered information that led them to not hire a candidate.[18] When user-generated content and information carries risks such as those stated above, it is not surprising that based on a September 2013 study conducted by the Pew Research Center,

> [Eighty–six percent] of adult Internet users have taken steps from time to time to avoid surveillance by other people or organizations when they were using the Internet. Despite their precautions twenty-one percent of online adults have had an email or social media account hijacked and eleven percent have had vital information like Social Security numbers, bank account data or credit cards stolen—and a growing number worry about the amount of personal information about them that is available online.[19]

Many users question exactly what role or liability social networking providers assume for protecting users against such risks—sadly, the

---

17 *Id*.; *see also* Katherine Hutt, *Imposter Facebook Profiles Can Fake Out Your Real Friends*, BETTER BUSINESS BUREAU, http://www.bbb.org/blog/2013/07/imposter-facebook-profiles-can-fake-out-your-real-friends/ (Reporting an increasing number of reports regarding fraudulent Facebook accounts where third parties use another person's name, photographs, or other identifying information for improper uses).

18 *More Employers Find Reasons Not to Hire Candidates on Social Media, Finds CareerBuilder Survey*, CAREERBUILDER (June 27, 2013), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2013&id=pr766&ed=12%2F31%2F2013.

19 Lee Rainie et al., *Anonymity, Privacy, and Security Online,* PEW RESEARCH CENTER (Sept. 5, 2013), http://www.pewinternet.org/~/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf.; *see also* Bruce Drake, *What Strategies Do You Use to Protect Your Online Identity?*, PEW RESEARCH CENTER (Sept. 5, 2013) http://www.pewresearch.org/fact-tank/2013/09/05/what-strategies-do-you-use-to-protect-your-online-identity/ (provides a list of strategies that adult internet users have used to protect their online identity).

answer is not much. While Facebook and Twitter provide standard privacy settings to protect users' confidential information online,[20] there are several reasons why these mechanisms often fail to provide the privacy protection that many users desire.

B. *Social Media Networks Immune from Liability*

Social media networks such as Facebook, have few incentives to protect the interests of individual users, largely because "Section 230 of the Federal Communications Decency Act (CDA), which states that 'no provider . . . shall be treated as the publisher or speaker of any information provided by another content provider' . . . granting every Internet service provider (ISP) immunity from liability for defamation and invasion of privacy."[21] Similarly, in *Barnes v. Yahoo! Inc.*, the Ninth Circuit Court of Appeals barred plaintiff's action against Yahoo! under Section 230(c)(1) and (e)(3) of the Communications Decency Act based on a finding that Yahoo! was a non-publisher or speaker of third-party generated content.[22] The law in this regard favors social media providers and ISPs by eliminating any liability for user-generated content shared on their websites and further enables them to, "[M]onetize the rich trove of data [they] collect from [their] users"[23] to increase overall advertising revenue. As a result, today's digital landscape remains ripe with opportunities for one's identity to be maliciously misappropriated, and historically there has been minimal recourse available for impersonation via social media, online postings or email.[24]

Huffington Post contributor Janet Tavakoli, a victim of online impersonation, detailed her experience in trying to end her perpe-

---

[20] *Privacy*, FACEBOOK, https://www.facebook.com/help/445588775451827 (last visited Nov. 3, 2013).

[21] Neville L. Johnson, *Remedies for Web Defamation,* CALIFORNIA LAWYER (May 2013), http://www.callawyer.com/clstory.cfm?eid=928446&wteid=928446_Remedies_for_Web_Defamation.

[22] Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009) (plaintiff's claim against Yahoo for third-party publication of nude photographs and her workplace contact information was held not actionable; Yahoo immune from liability in accordance with Communications Decency Act § 230).

[23] Joe Nocera, Op-Ed., *Facebook's New Rules*, N.Y. TIMES (Oct. 18, 2013), *available at* http://www.nytimes.com/2013/10/19/opinion/nocera-facebooks-new-rules.html?_r=0.

[24] Yakub Hazzard & Dan Stone, *A Little Known Weapon to Combat Online Impersonation: California Penal Code Section 528.5*, ROBINS, KAPLIN, MILLER & CIRESI LLP, (May 23, 2012), http://www.rkmc.com/~/media/PDFs/A%20Little%20Known%20Weapon%20to%20Comba%20Online%20Impersonation.pdf.

trator's fake online presence. In a series of articles, Tavakoli explains how Facebook's business model, terms and conditions, and privacy settings may at first glance appear to offer protection from cybercrimes, but often fail to effectively safeguard against such abuses. Ironically, in order to gain control over the fraudulently created account Tavakoli was required to provide Facebook with confidential identifying information, while her impersonator effectively remained anonymous. She writes:

> In its disclosures, Facebook never specifically mentions the word "impersonator" i.e., identity thief. I found that personally interesting, because as I wrote in July 2011, someone put up a fake profile of me. Thanks to Google Alerts, I discovered the problem. In order to get it removed, I had to prove my identity to Facebook with a government-issued I.D., yet the identity thief didn't have to prove anything at all to create the fake. I didn't want to fork over personal information to Facebook, but the alternative was that a fraudster might use the fake profile maliciously.[25]

Tavakoli, like many victims, highlights the frustrating and often tedious process of resolving online impersonation disputes with social media providers directly. Facebook has terms and conditions to guard against online impersonation, however the process of reporting a violation on their platform routes users through a series of survey-like questions intending to streamline the reporting process. For a website that prides itself on its community brand image, Facebook's reporting process is, quite frankly, laissez-faire. Although this may disturb and frustrate many users, the law simply does not require Facebook to take more than minimal precautions.

While the enactment of online impersonation statutes is a proactive step in helping to deter and remedy such cases, a myriad of barriers to effective enforcement remain. It can be difficult to identify an anonymous online perpetrator, the ubiquity of the Internet raises jurisdictional issues, and in some instances, interpretation of the statutes themselves make these cases hard to prosecute.[26] For example, under California's impersonation statute[27] terms such as "harming another person" and "other elec-

---

[25] Janet Tavakoli, *Facebook's Fraud Problem Worse than it Appears in Disclosures*, HUFFINGTON POST (Nov. 26, 2012 at 6:33am), http://www.huffingtonpost.com/janet-tavakoli/facebooks-fraud-problem-w_b_2190575.html.

[26] Mark Hansen, *NJ Woman Can Be Prosecuted Over Fake Facebook Profile, Judge Rules*, A.B.A. JOURNAL (Nov. 4, 2011), http://www.abajournal.com/news/article/woman_can_be_prosecuted_over_fake_facebook_profile_judge_rules/.

[27] CAL. PENAL CODE § 528.5 (West 2011).

tronic means" leave ambiguity as to exactly what conduct or digital platform the law applies.[28] Thus, the need for time-efficient and cost-effective legal remedies is ever-present.

II. Legal Foundations of Online Impersonation Law

A. *Cyberbullying Raises Awareness of Other Cyber-Related Crimes*

In *United States v. Drew*[29] the issue of cyberbullying came to the forefront after a thirteen-year-old girl, Megan Meier, committed suicide in a St. Louis suburb in 2006. It was later revealed that she had been targeted online by a fictitious thirteen-year-old boy whose MySpace page had been created by the mother of another teenage girl. Prosecutors discovered that Lori Drew sought to humiliate Meier because she suspected that Meier had spread rumors about her teenage daughter. Drew was convicted on three misdemeanor counts of accessing computers without authorization, but a federal judge in 2009 threw out the convictions. At the time of Meier's case, "Missouri prosecutors did not have the necessary tools to prosecute Lori Drew, so the federal government decided to step in and charge her in California. Eventually those charges were overturned."[30] While cyberbullying legislation and educational initiatives have been steadily adopted and implemented nationwide to prevent more cases like Meier's from happening, state legislatures have largely been slow to adopt legal remedies for victims of online impersonation. Subdivision B below, further explains how cyberbullying and online impersonation differ in statutory definition and the scope of available legal recourse for victims.

---

28 Hazzard & Stone, *supra* note 24.

29 259 F.R.D. 449 (C.D. Cal. 2009).

30 Christopher S. Burrichter, Comment, *Cyberbullying 2.0: A "Schoolhouse Problem" Grows Up*, 60 DePaul L. Rev. 141, 146 (2010).

B. *Online Impersonation – Distinct from Cyberbullying and Identity Theft*

1. Cyberbullying

Online impersonation occupies a gray area in the law[31] that relates to cyberbullying, identity theft, and, at times, criminal law, making it difficult to understand where one area ends and other should begin. Generally, online impersonation is considered a form of cyberbullying, which exists among other forms such as e-mail hacking and cyberstalking.[32] According to Enough Is Enough (EIE), a non-partisan, 501(c)(3) non-profit organization and national leader in the area of Internet safety for children and families, 43% of teens aged thirteen to seventeen report that they have experienced some sort of cyberbullying in the past year.[33] It helps to think of cyberbullying as an umbrella term that encompasses a broad range of impermissible online conduct often discussed in the context of education. Cyberbullying takes traditional teasing and bullying among schoolchildren on the playground to a wider, more pervasive online context, which in turn, has led to serious and life-threatening consequences among today's youth. For example, in New York cyberbullying is statutorily defined as harassment or bullying that has the effect of creating a "hostile environment by conduct or by threats, intimidation or abuse . . . that would have the effect of unreasonably and substantially interfering with a student's educational performance, opportunities or benefits, or mental, emotional or physical wellbeing."[34]

2. Cyberstalking

In the case of cyberstalking, which is a more serious form of cyberbullying, the laws are intended to prevent threatening online

---

31 Donna Engle, *Legal Matters: Online Impersonation a Gray Area Legally*, CARROLL COUNTY TIMES (July 28, 2013, 12:00 AM), http://www.carrollcountytimes.com/columnists/features/law/legal-matters-online-impersonation-a-gray-area-legally/article_3f41da5e-9fd7-57a7-9386-53068cc3c107.html.

32 Allison Van Dusen, *How to Stop Cyber-Bullying*, FORBES (Sept. 15, 2008, 6:15 PM), http://www.forbes.com/2008/09/15/bully-school-cyber-forbeslife-cx_avd_0915health.html.

33 *Online Bullying*, ENOUGH IS ENOUGH, http://internetsafety101.org/cyberbullying.htm (last visited Nov. 3, 2013).

34 N.Y. EDUC. LAW § 7(a); *see also*, N.Y. EDUC. LAW § 7(b)-(d); Buzzfeed Staff, *9 Teenage Suicides in the Last Year Were Linked to Cyber-bulling on Social Network*, BUZZFEED (Sept. 11, 2013, 4:34 PM), http://www.buzzfeed.com/ryanhatesthis/a-ninth-teenager-since-last-september-has-committed-suicide (reporting nine cases of cyber-bulling that led to suicide among affected teenagers within the last year).

conduct where the victim is likely to fear for his or her own physical safety or life due to the conduct of the perpetrator or related third-party.[35] Accordingly, the National Conference of State Legislatures defines cyberstalking as, "[T]he use of the Internet, email or other electronic communications to stalk, and generally refers to a pattern of threatening or malicious behavior. Cyberstalking may be the most dangerous of the types of Internet harassment based on posing a credible threat of harm."[36] If placed on a spectrum from least to most dangerous, online impersonation would come before cyberstalking because the degree of foreseeable harm is most often, less likely to place the victim in reasonable fear for his or her own safety.

3. Identity Theft

Lastly, identity theft differs from online impersonation to the extent that the underlying motivation of the perpetrator is often to financially benefit from the use of his victim's confidential information. According to the U.S. Department of Justice, an individual's Social Security number, bank account or credit card, and other valuable personal data are often used by a perpetrator to illegally profit at their victim's expense.[37] In comparison, AllClearID, an identity protection technology company, points out that online impersonation is often more difficult to prevent because a perpetrator only needs a person's name, telephone number or email address to impersonate them online.[38] However, "the aftermath of identity theft is often much more far-reaching than that of online impersonation,"[39] and its victims may incur substantial out-of-pocket losses and expenses associated with efforts to clear their name and rectify reputational damage caused by the perpetrator.[40]

---

35 Emily D. Walterscheid, *Cyberstalking and Impersonation*, MATTHEW HARRIS LAW (Aug. 5, 2013) http://blog.matthewharrislaw.com/index_files/CyberstalkingandImpersonation.htm.

36 *"State Cyberstalking and Cyberharassment Laws,* NCLS.ORG, http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx (last visited Dec. 8, 2013).

37 *Identity Theft and Identity Fraud: What Are Identity Theft and Identity Fraud?*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/fraud/websites/idtheft.html (last visited Feb. 4, 2014).

38 *Online Impersonation vs. Identity Theft: Is there a Difference?*, ALLCLEAR ID (Dec. 17, 2012), https://www.allclearid.com/blog/online-impersonatin-vs-identity-theft.

39 *Id*.

40 U.S. DEP'T OF JUSTICE, *supra* note 37.

C. *What is online impersonation?*

In Texas, a local reporter pled guilty to online impersonation for using the names of two college football players to solicit sexual conduct from married women and teenage girls online.[41] Likewise, in California, a teenager was sentenced to not more than a year in juvenile detention after he admitted to accessing a classmate's Facebook profile, altering the content and posting sexually explicit messages on two of her male friends' profiles.[42] Using the foregoing cases as examples, one can see that online impersonation extends beyond the normative context of cyberbullying among adolescents and spans the gamut to affect social media and Internet users both young and old across a variety of contexts. For example, in *Draker v. Schreiber*,[43] an assistant principle tried to bring a suit against two of her students after they created a fake profile of her, but failed to assert a specific cause of action that appropriately addressed the type of harm she had suffered.[44] Justice Stone, presiding over the Fourth Circuit Court of Appeals in Texas, asserted in her concurring opinion, "There appears to be little civil remedy for the injured targets of these Internet communications . . . The citizens of Texas would be better served by a fair and workable framework in which to present their claims, or by an honest statement [because] there is, in fact, no remedy for their damages."[45]

Since then, three leading jurisdictions, California, New York, and Texas have enacted legislation to specifically criminalize online impersonation (also known as "e-personation") via electronic communication. Others including Hawaii, New Jersey, Arizona, and Missouri have either proposed entirely new legislation or enacted amendments to existing harassment or identity theft laws to include such conduct.[46] State online impersonation statutes across

---

41 Rodolfo Ramirez, *Online Impersonation: A New Forum for Crime on the Internet*, 27 No. 2 AM. BAR ASS'N 6 (Summer 2012), *available at* http://www.americanbar.org/content/dam/aba/publications/criminal_justice_magazine/CJ_Summer2012.authcheckdam.pdf; *see* State v. Georgandis, No. 10-DCR-055790 (Tex. Crim. Dist. Nov. 18, 2011), *available at* http://tylerpaw.co.fort-bend.tx.us/CaseDetail.aspx?CaseID=1024938).

42 *In re* Rolando S., 129 Cal. Rptr. 3d 49, 52 (Ct. App. 2011), *available at* http://cases.laws.com/california-in-re-rolando-s-7-21-11-ca5.pdf.

43 Draker v. Schreiber, 271 S.W.3d 318, 324 (Tex. App. 2008).

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

45 *Draker*, 271 S.W.3d at 327.

46 Amy Coleman, *Catfish Season*, DUQ. UNIV. SCH. OF LAW JURIST NEWS MAGAZINE (Apr. 19, 2013), http://duquesnejurismagazine.blogspot.com/2013/04/catfish-season.html.

various jurisdictions largely incorporate similar key elements: (1) impersonation without the victim's consent, (2) via an electronic communication channel such as social networking sites, email, text message, among others, and (3) the perpetrator must act with the intent to harm, intimidate, threaten or defraud. However, states differ as to whether such conduct constitutes a misdemeanor or felony offense, and legal professionals have questioned whether existing cyber harassment and identity theft laws are sufficiently broad enough to be applied to online impersonation cases; thus eliminating the need to adopt new statutes all together.[47] While the above cases exemplify that online impersonation statutes have led to successful prosecution in various states, their application largely hinges on the plain reading of each state's statute.

D. *Analysis of Currently Enacted State Online Impersonation Statutes*

Currently, only California,[48] Texas,[49] New York,[50] Mississippi,[51] and Hawaii[52] have statutes that explicitly contain language referring to "online impersonation."[53] In the subsections below, the California, Texas, and New York statutes are discussed in greater detail given their recognition as leading U.S. jurisdictions and the wealth of supporting commentary regarding their enactments. There are also several jurisdictions including New Jersey[54] and Arizona,[55] among others, who have proposed legislation that specifically outlaw online impersonation. Legislation from Mississippi, Hawaii, New Jersey, and Arizona will be further discussed in Part III – Barriers to Imposing Liability.

---

47 Anita Ramasastry, *Dealing with E-Personation: A Recent New Jersey Case Shows Why New Laws Aren't Really Needed to Address Fake Facebook Profiles and the Like*, JUSTIA.COM (Nov. 22, 2011), http://verdict.justia.com/2011/11/22/dealing-with-e-personation.

48 CAL. PENAL CODE § 528.5 (West 2011).

49 TEX. PENAL CODE ANN. § 33.07 (West 2011).

50 N.Y. PENAL LAW § 190.25(4) (McKinney 2008).

51 MISS. CODE ANN. § 97-45-33 (West 2011).

52 HAW. REV. STAT. § 711-1106.6 (West 2008).

53 Jonathan Bick, *Internet Law: Some States Criminalize Internet Identity Theft*, NJLJ (Nov. 18, 2013), http://www.bracheichler.com/C3F493/assets/files/News/Bick%2011.18.13.pdf.

54 NJ Assembly Bill Approved: http://legiscan.com/NJ/bill/A2105/2012.

55 H.R. 2004, 51st Leg., 1st Reg. Sess. (Ariz. 2012), *available at* http://legiscan.com/AZ/text/HB2004/id/670151.

1. California

California's online impersonation statute, codified as CAL. PENAL CODE § 528.5, was enacted in 2010 (effective January 1, 2011) in large part because of the advocacy set forth by State Senator Joe Simitian. Simitian was motivated to help enact legislation after Carl Guardino, the chief executive officer of the Silicon Valley Leadership Group, became a victim of online impersonation when a third-party perpetrator sent out emails using his name to defame a news reporter.[56] As in *Draker,*[57] California had no claim to properly address Guardino's claim. An act to add Section 528.45 to the Penal Code, relating to impersonation, was filed with the Secretary of State on September 27, 2010 and became effective January 1, 2011.[58] In a fact sheet submitted to the California State Senate, Simitian explained that passage of then Senate Bill 1411, was intended to update, "existing law addressing impersonation [that] was written in 1872, without the modern technologies of today in mind."[59] It was further noted that the law was intended to "expand the current impersonation statute to include impersonation done on an Internet website or through other electronic means such as email, Facebook, Twitter, and other social media websites."[60]

Subdivision (a) requires that the perpetrator "credibly" impersonate another person on an Internet website or by other electronic means with the intent to harm, intimidate, threaten, or defraud another person.[61] A credible impersonation as defined by subdivision (b) occurs if "another person would *reasonably believe*, or did reasonably believe, that the defendant was or is the person who was impersonated."[62] In addition, the California legislature specifically provided that "electronic means" in subdivision (a) also prohibits a perpetrator from opening an e-mail account in the victim's name, not just an account or profile via a social networking site; this designation is unique to California's statute.[63] Further, a credible impersonation based on subdivisions (a) and (b) consti-

---

56 Videotape: Nigam on CNN Newsroom, YOUTUBE (January 3, 2011), http://www.youtube.com/watch?v=XHRHuFPK45c.

57 Draker v. Schreiber, 271 S.W.3d 318, 324 (Tex. App. 2008).

58 CAL. PENAL CODE § 528.5 (West 2011).

59 Sen. Joseph Simitian, *Fact Sheet: Senate Bill 1411 (Simitian) Criminal "E-Personation"*, STATE SENATOR JOE SIMITIAN, http://www.senatorsimitian.com/images/uploads/SB_1411_Fact_Sheet.pdf (last visited Nov. 2, 2013).

60 *Id*.

61 CAL. PENAL CODE § 528.5(a).

62 *Id.* at § 528.5(b).

63 *Id.* at § 528.5(c).

tutes a misdemeanor offense punishable by a fine not exceeding $1000, or by imprisonment not to exceed one year, or both fine and imprisonment.[64] In addition, compensatory damages and injunctive relief or other equitable relief pursuant to the statute may be imposed.

In October of 2011, California achieved its first conviction under the state impersonation statute[65] when, Jesus Felix, a twenty-two year-old Los Angeles resident confessed to posting sexually explicit photographs of his ex-girlfriend across a myriad of 130 fraudulent Facebook pages and Craigslist listings he created.[66] After pleading guilty to two-counts of "e-personation," Judge Yvette Verestegui ultimately sentenced Felix to five years probation and thirty days of community service work.[67] In yet another early case filed on July 21, 2011, defendant Rolando S. evaded conviction under CAL. PENAL CODE § 528.5 since he committed the impersonation before the new statute was officially in effect.[68] However, Judge George L. Orndoff of the 5th District Court of Appeals affirmed his conviction under another related statute, CAL. PENAL CODE § 530.5, which outlaws the unauthorized use of personal information of another person.[69] This case is noteworthy because of the statutory analysis Judge Orndoff provides in the footnotes of the opinion, which drive home the critical distinction between § 528.5 and § 530.5.[70] Unlike § 530.5, § 528.5 does not require the defendant to willfully obtain the victim's personal information or the intent to act with an unlawful purpose.[71] Thus, a person may be liable under § 528.5 for merely coming into possession of one's

---

64 *Id.* at § 528.5(d).

65 *Id*.

66 Office of the City Attorney: Los Angeles, Cal., Press Release: City Attorney's Office Secures First Conviction Under New Internet Impersonation Law (Oct. 19, 2011), http://www.atty.lacity.org/stellent/groups/electedofficials/@atty_contributor/documents/contributor_web_content/lacityp_015740.pdf.

67 Ramasastry, *supra* note 47, at 3.

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

69 CAL. PENAL CODE § 530.5.

70 *Id.* at §§528.5, 530.5.

71 *In re* Rolando S., 129 Cal. Rptr. 3d at 9 (We note, however, that section 530.5 has different elements from section 528.5. Section 530.5 requires that a person willfully obtain personal identifying information and use it for an unlawful purpose. Section 528.5 does not include a requirement that a perpetrator obtain personal identifying information. As a result, a person could violate section 528.5 by merely posting comments on a blog impersonating another person. There is no requirement, under these circumstances, that the person obtain a password—a key distinction.

Further, section 528.5 does not require the perpetrator act with an unlawful purpose—merely that he or she acted with the purpose of harming, intimidating, threatening, or defrauding

personal information and using it to harm, intimidate, threaten or defraud another in any way.[72]

2. Texas

Unlike California's statute, which expressly makes online impersonation a misdemeanor, online impersonation under Texas law can constitute either a misdemeanor or felony offense depending on whether the perpetrator acted *with or without* malicious intent.[73] The statute was enacted as Texas Penal Code § 33.07 in 2009 and amended in 2011 in order to change the statute's title from "Online Harassment" to "Online Impersonation."[74] Under the statute there are two scenarios in which a person may be charged with the crime of online impersonation. The conduct enumerated in subdivision (a)[75] constitutes a third-degree felony, whereas subdivision (b)[76] sets out conduct sufficient to constitute a Class A misdemeanor. As Fort Bend County, Texas Assistant District Attorney, Rodolfo Ramirez, points out, "Subsection (a) makes it a violation to use the name or persona of another person; it does not limit it to using an identical match."[77] Thus, the statute is effectively broad enough to be applied to cases in which the victim's persona or photographs are used to create a social media profile even under a fake name.

---

a person. At least the terms "harming" and "intimidating" do not necessarily have to be done for an unlawful purpose.

The act of willfully obtaining someone else's password, and then using it for an unlawful purpose, justifies more harsh treatment under section 530.5. We believe if appellant had committed these same acts after January 1, 2011, he could have been charged under both sections 528.5 and 530.5.).

72 CAL. PENAL CODE § 530.5 (West 2011).

73 TEX. PENAL CODE ANN. § 33.07 (West 2011).

74 *Id*.

75 TEX. PENAL CODE ANN. § 33.07(a) (Online impersonation constitutes a third-degree felony where: (a) 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 networking site or other Internet website, other than on or through an electronic mail program or message board program).

76 TEX. PENAL CODE ANN. § 33.07(b) (Online impersonation constitutes a Class A misdemeanor where: (b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person: (1) without obtaining the other person's consent; (2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and (3) with the intent to harm or defraud any person).

77 Ramirez, *supra* note 41, at 2.

Based on the statutory language of subdivisions (a) and (b), there are two significant differences between the felony and misdemeanor conduct. First, the misdemeanor offense under subdivision (b) merely requires that the perpetrator engage in the *distribution* of another's identifying information, whereas the felony charge under subdivision (a) requires the *creation of a web presence* using the victim's name or persona.[78] Second, the misdemeanor does not require that the perpetrator act with the intent to intimidate or threaten; but merely that he or she attempted to harm or defraud the victim.[79] In addition, the statute specifically enumerates an exception in which misdemeanor conduct under subdivision (b) may rise to constitute, "a felony of the third degree if the actor commits the offense with the intent to solicit a response by emergency personnel."[80] Lastly, subdivisions (e)(1–5) indemnify commercial, social networking sites, Internet service providers, interactive computer services, telecommunication providers, and video service providers and thus aligns with federal statutes such as the Anticybersquatting Consumer Protection Act (15 U.S.C. Section 1125), and the Uniform Domain-Name Dispute-Resolution Policy (UDRP) which will be further discussed in a Section IV.

As recent as January 16, 2014, Victoria Varnes, an eighteen-year-old University of Texas Arlington student, was arrested on charges of online impersonation after she created a website featuring provocative photographs under another person's name.[81] Pursuant to the Texas Penal Code,[82] online impersonation is a third-degree felony, and if convicted, Varnes faces a maximum fine of $10,000 or imprisonment of up to ten years. While the case is currently awaiting trial, an affidavit filed with the court revealed that Varnes attempted to make an emotional plea to the victim in a handwritten apology letter stating, "I'm sorry my actions have caused you personal embarrassment. It wasn't my intention to harm you in any way or impersonate you. It is unfortunate that I chose a screen name that may be confused with yours."[83]

Similarly, City Councilwoman Stacie Keeble became an online impersonation victim when her husband's former personal assis-

---

78 TEX. PENAL CODE ANN. § 33.07(a)-(b)(1-3) (West 2011).

79 *Id.* at § 33.07(b)(1-3).

80 *Id.* at § 33.07(d).

81 Rafael Sears, *Student Faces Online Impersonation Charge,* THE SHORTHORN, (Jan. 16, 2014, 10:30 AM, updated 11:43 AM), http://www.theshorthorn.com/news/student-faces-online-impersonation-charge/article_66512bfe-7e56-11e3-b9c0-001a4bcf6878.html.

82 TEX. PENAL CODE ANN. § 33.07 (West 2011).

83 Sears, *supra* note 81.

tant, who had access to their family photographs, created a fraudulent Facebook page featuring pictures of her head attached to another woman's naked body.[84] Defendant, Chris Zamarripa, pled guilty to the felony charge of online impersonation.[85] He "blamed his actions last January on being drunk and upset with Robert Keeble, Stacie's husband, for whom he [had] worked [with] since 2007 until a falling out last October."[86] Zamarripa accepted a plea deal of a $2,500 fine and five years of deferred adjudication probation since he had no previous criminal record.[87]

3. New York

New York's online impersonation law is codified at N.Y. Penal Law § 190.25(4). Subdivision (4) was added to § 190.25, which generally governs criminal impersonation in the second degree, and became effective on November 1, 2008.[88] New York State Senator Andrew Lanza (R-Staten Island) originally introduced the online impersonation legislation, (S.4053), in April 2007.[89] In advocating for the law, Lanza noted, "The problem of Internet impersonation is intensifying with the growing availability of personal data online, as well as the increase in social networking and dating sites. Internet imposters are finding ways to defraud and victimize people . . . [w]e must address the growing danger posed by Internet imposters by passing the law."[90] Similar to California, online impersonation in New York constitutes only a class A misdemeanor punishable by imprisonment up to one year and a fine of up to $10,000. Under Section § 190.25(4), a person is guilty of criminal online impersonation in the second degree when he or she impersonates another by communicating on an Internet website or electronic means with the intent to obtain a benefit, injure or defraud another.[91] Additionally, a person who by such communication pretends to be a public servant in order to induce another to submit to

---

84 Zeke Maccormack, *Phony Facebook Page Targeted Kerrville City Council Member*, SAN ANTONIO EXPRESS NEWS (Oct. 9, 2013, 10:53 PM), *available at* http://www.mysanantonio.com/default/article/Phony-Facebook-page-targeted-Kerrville-City-4882480.php.

85 *Id*.

86 *Id*.

87 *Id*.

88 S. 4035, Ch. 304, 2008 Leg., 231st Sess. (N.Y. 2008).

89 Andrew J. Lanza, *Senator Lanza Introduces Legislation Making Internet Impersonation a Crime*, NYSenate.gov (Apr. 4, 2007), http://www.nysenate.gov/news/senator-lanza-introduces-legislation-making-internet-impersonation-crime.

90 *Id*.

91 N.Y. PENAL LAW § 190.25(4) (McKinney 2008).

such authority or act in reliance on such pretense is also liable under the statute.[92]

A memorandum originally accompanying the New York State Assembly bill provides that "the purpose of the new law [was] to deter perpetrators who, with intentions ranging from harassment to identity theft, gain access to another person's account and pose as them through the use of online communications."[93] Attorneys at Hunton & Williams law firm in New York note that the actual scope of conduct that the law may be applied to is likely even broader than the legislature's stated purpose.[94] By its plain language, the law applies to any person or entity that impersonates another person on the Internet . . . the new law is intended to "deter the plethora of cases [of] misrepresenting oneself through the use of the Internet."[95] However, if litigation under the specific online impersonation statute were to fail, New York has either its identity theft statute, N.Y. Penal Law § 190.77–.80, or its harassment statutes, N.Y. Penal Law § 240.25 et. seq.[96]

III. Effectiveness of Current Online Impersonation Statutes

The enactment of statutes aimed to combat the harmful effects of online impersonation constitutes progressive state reform. However, even if these leading jurisdictions provide a possible effective legal solution for other states to replicate, the majority of U.S. jurisdictions have yet to follow suit. Currently enacted statutes are limited in their effectiveness for numerous reasons. Bars to effective resolution of online impersonation are present at all stages of the litigation process.

---

92 *Id*.

93 Hunton & Williams, *Client Alert: New York Makes Internet Impersonation a Crime*, (Dec. 2008), http://www.hunton.com/files/News/dfa38a93-b157-4c1c8965c46ee50f15a4/Presentation/NewsAttachment/7aac8c6f-3705-403e-9be96dabf858f83e/new_york_internet_impersonation_privacy_alert.pdf.

94 *Id*.

95 *Id*.

96 Ramirez, *supra* note 41, at 4–5.

A. *Barriers to Imposing Civil and/or Criminal Liability*

1. Cost of Litigation

In January 2013, the National Center for State Courts released a report estimating the average cost of civil litigations. For example, a typical automobile tort case resolved shortly after initiation ranges from $1000 at the twenty-fifth percentile to $7350 at the seventy-fifth percentile and requires a minimum of 96.5 professional hours.[97] As expected, the total cost of legal fees substantially increases as the case proceeds through discovery, settlement, pre-trial, trial, and post-disposition phases. Accordingly, a case that results in a settlement after discovery has been completed either through traditional settlement negotiations or the use of ADR methods ranges from $5000 to $36,000.[98] Unsurprisingly, the cost of a case litigated through the trial stage will further range from $18,000 to $109,000 per side.[99] When contrasted against the fact that Facebook is most appealing to eighteen to twenty-nine year olds,[100] the likelihood that such users will be able to afford and successfully litigate a case of online impersonation seems incredibly bleak.

2. Difficulty Identifying an Anonymous Perpetrator

Once, and even if litigation is sought, the plaintiff bears a heavy burden of identifying his or her alleged perpetrator because cyber crimes enable perpetrators to maintain greater anonymity and further difficulties may arise when proving the perpetrator's alleged intent. Michael D. Scott, a leading expert on technology and business law and author of the treatise, *Scott on Information Technology*, outlined several additional factors regarding cyber crimes that make them more difficult to litigate. These include:

> (1) The anonymous nature of many online activities allows cybercriminals to mask their identity, (2) cybercrimes can be achieved from virtually anywhere in the world, as long as there is Internet access, (3) technology can be used to hide the crimi-

---

97 Paula Hannaford-Agor & Nicole L. Waters, *Case Highlights: Estimating the Cost of Civil Litigation*, COURT STATISTICS PROJECT (Jan. 2013) http://www.courtstatistics.org/~/media/microsites/files/csp/data%20pdf/csph_online2.ashx.

98 *Id*.

99 *Id*.

100 Shea Bennett, *Facebook, Twitter, Pinterest, Instagram – Social Media User Demographics 2013*, MEDIABISTRO (Apr. 15, 2013, 6:00AM), http://www.mediabistro.com/alltwitter/social-user-demographics_b39963.

> nal activity and delay or even prevent the victim from learning of the crime, and (4) the size of the Internet provides an enormous pool of potential victims of these crimes.[101]

Such factors make litigating cases of online impersonation substantially harder to resolve than those where the perpetrator's identity is known; but social media, cellular phone providers or website administrators can be subpoenaed for this information where needed.[102]

3. Jurisdictional & Choice of Law

In 2012, online impersonation charges brought under Texas law were later dismissed for lack of jurisdiction over Adam Limle, an Ohio resident.[103] Limle allegedly created a website depicting photographs of his former girlfriend, a Texas resident, as a prostitute. As the first case brought under Texas' new online impersonation law, Texas legislators and Travis County prosecutors failed to foresee the jurisdictional limits of the law that were later raised by Limle's defense attorney to dismiss the case.[104] The problem lies in the fact that the computer software that Limle used to create the website was located not in Texas, but at his residence in Ohio. John Lopez, Travis County prosecutor, commented on the case saying, "The Internet crosses state and international boundaries and we have such a mobile society people moving from country to country, state to state . . . you could affect somebody's life in another part of the world and not set foot in that country and how do you deal with those kinds of offenses?"[105]

Indeed, this case raises exactly the type of concerns that Anita Ramasastry, professor at the University of Washington School of Law, warned of when advocating against the enactment of online impersonation statutes.[106] According to Ramasastry, legislators risk unforeseen issues when they attempt to "create new laws in response to changing technological phenomena, there is always a risk that the law will be outdated quickly, will not properly capture

---

101 MICHAEL D. SCOTT, *Cybercrimes*, in SCOTT ON INFORMATION TECHNOLOGY § 17.11 (2012).

102 *Law Enforcement and Third Party Matters,* FACEBOOK https://www.facebook.com/help/473784375984502/ (last visited Jan. 27, 2014).

103 *Online Impersonation Charged Dropped Due to Loophole*, MY FOX AUSTIN (May 21, 2012, 6:27 PM), http://www.myfoxaustin.com/story/18670402/online-impersonation-charged-dropped-due-to-loophole.

104 *Id*.

105 *Id*.

106 Ramasastry, *supra* note 47.

all intended acts, and will cover acts that are already illegal or that already give rise to civil claims under common law or other statutes."[107] Ramasastry's main argument is that the enactment of specific online impersonation statutes is not needed where a state's existing identity theft, cyberbullying, or harassment laws are already sufficient to prosecute online impersonators.[108] In Hawaii, for example, a victim of online impersonation could potentially bring an action under the state's 'Harassment by Impersonation' statute.[109] The statute employs extremely broad language by permitting a cause of action where a person, "[E]ither directly or indirectly causes, a transmission of *any* personal information of the person to another by *any* oral statement, *any* written statement, or *any* statement conveyed by *any electronic means*, with the intent to harass, annoy, or alarm any person."[110]

At first glance, Ramasastry's argument seems to add a degree of clarity to an otherwise ongoing and complex debate. Specific online impersonation laws seem like mere duplicates of laws that already exist, as in the case of Hawaii's statute. Similarly, there is a strong argument to simply amend the statutory language of an existing law to broaden the scope of impermissible conduct to that which may occur via "electronic communication" for example. The thinking is that if a victim of online impersonation has been harassed on a social media website or any other form of electronic communication, the underlying conduct is still harassment and the website, or e-mail for example, is merely the channel of communication. But, in contrast, legislators may risk providing no protection at all if they merely try to apply and/or amend old laws to fit today's new challenges.

The 2011 case of Dana Thornton strongly exemplifies both sides of the argument. In New Jersey, Thornton was prosecuted for

---

107 *Id*. at 3.

108 *Id*.

109 HAW. REV. STAT. § 711-1106.6 (West 2008)

> (1) A person commits the offense of harassment by impersonation if that person poses as another person, without the express authorization of that person, and makes or causes to be made, either directly or indirectly, a transmission of any personal information of the person to another by any oral statement, any written statement, or any statement conveyed by any electronic means, with the intent to harass, annoy, or alarm any person. (2) Harassment by impersonation is a misdemeanor. (3) For the purposes of this section: "Personal information" means information associated with an actual person that is a name, an address, a telephone number, or an electronic mail address. "Pose" means to falsely represent oneself, directly or indirectly, as another person or persons.

Id.

110 *Id*.

fourth degree identity theft after she created a fake Facebook profile for her ex-boyfriend, a narcotics detective, where she posted comments alleging that he frequently used drugs, had herpes, and engaged in sexual exploits with prostitutes.[111] At issue was N.J. Stat. Ann. § 2C:21-17(a)(1) which includes the following language: "(a) A person is guilty of an offense if the person: (1) Impersonates another or assumes a false identity and does not 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."[112] Defense Attorney Richard Roberts made all attempts to have Thornton's case dismissed by arguing that the law fails to make mention of Internet or any form of electronic communication. In a motion to dismiss the case, Roberts argued, "[I]n New Jersey, no courts have ever ruled that creating a profile of anyone online, without the individual's consent, constitutes false impersonation.[113] Attorney Roberts further commented, "Under the New Jersey statute, there is no plain wording, commentary, memorandum, or any evidence of legislative intent to show that impersonating someone online or by electronic means is a crime."[114] However, Judge David Ironson presiding over the State Superior Court believed otherwise, claiming that the law was "clear and unambiguous" by its terms and, "The fact that the means of communicating the crime are not set forth in the statute doesn't lead to the conclusion that the defendant didn't commit the crime."[115] Thus, Thorton's online impersonation case was allowed to proceed under New Jersey's identity theft statute absent a specific statutory reference to Internet communication, which exemplifies Ramasastry's argument that existing laws can provide resolution. In 2012, Thornton later agreed to participate in a pretrial intervention program consisting of fifty hours of community service and a psychological evaluation that if successfully completed would result in dismissal of her charges.[116]

---

111 Mark Hansen, *NJ Woman Can Be Prosecuted Over Fake Facebook Profile, Judge Rules*, A.B.A. JOURNAL (Nov. 4, 2011), http://www.abajournal.com/news/article/woman_can_be_prosecuted_over_fake_facebook_profile_judge_rules/.

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

113 Ramasastry, *supra* note 47, at 2.

114 *Id*.

115 David Porter, *Case of Fake Facebook Profile Can Proceed, Judge Rules*, LAW.COM (Nov. 3, 2011) http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202522461522&slreturn=20140109004110.

116 Ben Horowitz, *Bellville Woman Accused of Creating Fake Facebook Page to Mock Ex-Boyfriend Gets Probation*, NJ.COM (Mar. 19, 2012, 10:36 AM), http://www.nj.com/news/index.ssf/2012/03/belleville_woman_accused_of_cr_1.html.

Nevertheless, on January 17, 2014,[117] the New Jersey legislature approved an amendment to expand subdivision (a) of, N.J. Stat. Ann. § 2C:21-17, to include the following language: "A person is guilty of an offense if the person engages in one or more of the following actions by any means including, but not limited to, the use of electronic communications or an Internet website."[118] The amendment specifically clarifies that criminal impersonation can be committed via electronic communication and Internet websites.

4. First Amendment Concerns: Unconstitutionally Overbroad or Vague

In addition to jurisdiction and choice of law concerns stated above, online impersonation statutes have also faced a myriad of First Amendment challenges for being either unconstitutionally vague or overbroad and infringing on the constitutionally protected right to parody. In Arizona, Republican State Rep. Michelle Ugenti has strongly advocated for the enactment of legislation (H.B. 2004),[119] which would make online impersonation with the intent to harm, defraud, intimidate, or threaten another via social media or other forms of electronic communication a felony offense.[120] In addition, sending an email, text message, or instant message impersonating another person would constitute a misdemeanor offense.[121] Anjali Abraham, public policy director for the American Civil Liberties Union of Arizona, warns that any time proposed legislation concerns a First Amendment right, legislators must be cautious not to adopt language which sweeps too broadly and infringes upon protected forms of speech.[122]

Electronic Frontier Foundation (EFF), a nonprofit organization that defends civil liberties in the digital world, is one of the most recognized opponents against the enactment of online imper-

---

117 NJ Assembly Bill Approved, *available at* http://legiscan.com/NJ/bill/A2105/2012.

118 Bill Text: NJ A2105 Regular Session Amended.

119 H.B. 2004, 51st Leg., 1st Sess. (Ariz. 2013), *available at* http://www.azleg.gov/legtext/51leg/1r/bills/hb2004p.pdf.

120 Jim Cross, *Arizona Legislator Seeks Prison for Online Impersonation*, KTAR.COM (Jan. 7, 2013, 7:07 AM), http://ktar.com/22/1599856/Arizona-legislator-seeks-prison-for-online-impersonation.

121 Hunter Stuart, ARIZONA BILL COULD OUTLAW ONLINE IMPERSONATION, TWITTER PARODY ACCOUNTS, HUFFINGTON POST (Jan. 23, 2014, 6:58 PM), http://www.huffingtonpost.com/2013/01/04/arizona-bill-online-impersonation-twitter-parody-accounts_n_2409318.html?ncid=edlinkusaolp00000003.

122 Cindy Carcamo, *Arizona Legislator Targets Fake Twitter, Facebook Accounts*, L.A. TIMES (Jan. 9, 2013), *available at* http://articles.latimes.com/2013/jan/09/nation/la-na-nn-arizona-facebook-legislation-20130109.

sonation/e-personation legislation. EFF is concerned that such legislation has an unconstitutional chilling effect on the protected right to engage in political satire or parody.[123] Their main argument is that, "temporarily impersonating" corporations and public officials has become an important and powerful form of political activism, especially online."[124] Kurt Opsahl, senior staff attorney at EFF further commented saying, "The key is the 'intent to harm. . . [y]ou can imagine someone saying, "[W]ell, if you are making a parody of someone else and you are trying to make fun of them and hold them up to ridicule, that would be an attempt to harm them and thus would be within the coverage of the bill. That is the concern."[125]

Similar First Amendment concerns regarding overbreadth have been raised against a Missouri harassment statute, which may be applied to cases of online impersonation.[126] The statute outlines six ways in which a harassment offense may be committed. Subdivision (3) is likely the most applicable to a cause of action for online impersonation via social networks or other forms of Internet communication. Under the statute a person who, "[K]nowingly frightens, intimidates, or causes emotional distress to another person by anonymously making a telephone call or any electronic communication,"[127] commits the crime of harassment. However, the statute was recently challenged on First Amendment grounds in the case, *State v. Vaughn*, in which Judge William Ray Price Jr. of the Supreme Court of Missouri held that subdivision (5) was unconstitutionally overbroad on its face.[128] The constitutionality of subdivision (3) mentioned above was not at issue in this particular case, but the result in *Vaughn* does not preclude potential challenges that may arise in the future since the statute is comprised of six independent definitions of "harassment."[129]

---

123 Marie-Andree Weiss, *@Parody or @Crime? AZ Bill May Blur the Line*, DIGITAL MEDIA LAW PROJECT (Feb. 5, 2013), http://www.dmlp.org/blog/2013/parody-or-crime-az-bill-may-blur-line?utm_source=feedburner&utm_medium=feed&utm_campaign=feed%253A%2520CitizenMediaLawProject%2520%2528Citizen%2520Media%2520Law%2520Project%2529 (providing an overview of key First Amendment U.S. Supreme Court cases and related discussion of First Amendment concerns pertaining to Arizona's proposed bill).

124 Corynne McSherry, *"E-Personation" Bill Could be Used to Punish Online Critics, Undermine First Amendment Protections for Parody*, ELECTRONIC FRONTIER FOUNDATION (Aug. 22, 2010), https://www.eff.org/deeplinks/2010/08/e-personation-bill-could-be-used-punish-online.

125 Carcamo, *supra* note 122.

126 MO. ANN. STAT. § 565.090 (West 2012).

127 *Id.* at § 565.090(3).

128 State v. Vaughn, 3 66 S.W.3d 513, 520 (2012).

129 *Id.* at 520–21.

Due to the constant evolution of online communication and digital technology, state legislators who have yet to enact online impersonation legislation should be mindful that, "[T]he more specific the language, the more difficult it may be to prosecute such crimes."[130] For example, the plain language of Mississippi's online impersonation statute risks possible dismissal of cases for having too narrowly defined the scope of impermissible conduct. The statute, Miss. Code Ann. § 97-45-33,[131] defines "electronic means" as, "[T]he opening of an email account or an account or profile on a social networking Internet website in another person's name."[132] By narrowly defining electronic means as the 'opening of an email account or creation of a profile on a social network,' it seems possible that an imposter who creates a passive website with derogatory content that is not on a social media website could evade prosecution under the law.

5. Lack of Awareness of Legal Remedies

Lastly, as Facebook turns ten-years-old in 2014, there is no denying that it is the dominant social media website among U.S. users. A recent Pew Research Center study reported that 73% of online adults use a social networking site of some kind, among them a total of 71% are active Facebook users, representing a 4% increase in usage from the 67% of online adults who used Facebook in 2012.[133] In addition to being the most popular social media website among others by a margin of 49%,[134] Facebook also boasts the highest level of user engagement; a total of 63% of users

---

130 Ramirez, *supra* note 41, at 6.

131 MISS. CODE ANN. § 97-45-33 (West 2011).

> (1) Notwithstanding any other provision of law, any person who knowingly and without consent impersonates another actual person through or on an Internet website or by other electronic means for purposes of harming, intimidating, threatening or defrauding another person is guilty of a misdemeanor. (2) For purposes of this section, an impersonation is credible if another person would reasonably believe, or did reasonably believe, that the defendant was or is the person who was impersonated. (3) For purposes of this section, "electronic means" shall include opening an email account or an account or profile on a social networking Internet website in another person's name. (4) A violation of this section is punishable by a fine of not less than Two Hundred Fifty Dollars ($250.00) and not exceeding One Thousand Dollars ($1,000.00) or by imprisonment for not less than ten (10) days and not more than one (1) year, or both. (5) This section shall not preclude prosecution under any other provision of law and shall be considered supplemental thereto.

132 *Id.* at § 97-45-33(3).

133 Maeve Duggan and Aaron Smith, *Social Media Update 2013,* PEWINTERNET.ORG (Dec. 30, 2013) http://pewinternet.org/Reports/2013/Social-Media-Update/Main-Findings.aspx#footnote1.

134 *Id*.

visit the website at least one time per day, and 40% log on multiple times per day.[135] Yet, despite the high percentage of user engagement, Brenda Wiederhold, the editor-in-chief of the Journal of Cyberpsychology, Behavior, and Social Networking, points to high profile stories surrounding WikiLeaks and NSA surveillance procedures as the leading impetus for users choosing to opt out of the online world.[136] A research study published in the journal in 2012 revealed that among 48% of users who had committed "virtual identity suicide" by deleting their Facebook profiles, privacy concerns were their main reason for abandoning their online presence.[137] Even though privacy concerns continue to grow among users, Facebook and its social media counterparts still struggle to deter privacy breaches, which often lead to online impersonation disputes. Facebook has historically taken few proactive steps to help advocate and enforce their terms of service agreement, and reporting procedures for actual violations remain shielded behind a veil of a million clicks. Thus, in a society where no more than ten states have either specific online impersonation statutes or identity theft/harassment statutes that are broad enough to bring litigation, many users remain uniformed about online resources and available legal remedies to resolve such disputes.

In November 2013, U.S. Senator Sheldon Whitehouse of Rhode Island and Chair of the Senate Judiciary Committee on Crime and Terrorism, introduced legislation to promote increased public awareness of the need for cyber security and its potential threats to government, businesses and individuals alike.[138] Whitehouse noted that, "The cyber threat to American corporate and government networks and to individual users of the Internet is enormous and unrelenting . . . yet too many Americans remain in the dark about the severity and nature of this threat."[139] It seems as though the law is only just beginning to recognize the serious threat that e-personation poses to people of all ages; not just children. But the reluctance of most state legislators to enact tailored

---

135 *Id*.

136 Stefan Stieger, PhD., et. al., *Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addition and Personality Between Facebook Users and Quitters*, CYBERPSYCHOLOGY, BEHAV., AND SOC. NETWORKING (2012), http://online.liebertpub.com/doi/pdf/10.1089/cyber.2012.0323.

137 *Id*.

138 *Senators Introduce Legislations to Promote Public Awareness of Cyber Security*, SHELDON WHITEHOUSE: U.S. SENATOR FOR RHODE ISLAND, (Nov. 1, 2013), http://www.whitehouse.senate.gov/news/release/senators-introduce-legislation-to-promote-public-awareness-of-cyber-security.

139 *Id*.

legislation or provide cost and time efficient alternatives creates an environment where this conduct is allowed to persist and effective remedies are likely to lag behind. In such cases, Anita Ramasastry suggests that relying on reporting procedures created by the social media networks themselves could be a cost-effective and more effective solution to in-court litigation.[140] But, as the next section reveals, while reporting mechanisms are beneficial, they often fail to resolve the problem completely.

B. *Evaluating the Effectiveness of Social Media Providers' Online Dispute Procedures*

In November 2011, the Federal Trade Commission (FTC), the federal bureau responsible for preventing anticompetitive, deceptive and unfair consumer practices,[141] announced that Facebook agreed to settle FTC charges that it deceived users into believing their personal information could be kept private via the network's privacy control settings, but then repeatedly made this information publically available without their permission.[142] Among the FTC's eight-count complaint[143] against Facebook were the following findings:

> Facebook told users they could restrict sharing of data to limited audiences—for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used. Facebook promised users that it would not share their personal information with advertisers. It did . . . Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.[144]

---

140 Ramasastry, *supra* note 47, at 3.

141 *About the FTC*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/about-ftc (last visited Feb. 7, 2014).

142 *Facebook Settles FTC Charges that it Deceived Consumers By Failing to Keep Privacy Promises*, FEDERAL TRADE COMMISSION (Nov. 29, 2011), http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep (outlining the terms of Facebook's settlement agreement with the FTC).

143 Compl., *In the Matter of Facebook, Inc.*, FTC File No. 0923184 (2011) (No. C-4365), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

144 *Id*.

The settlement agreement finalized in August 2012, bars Facebook from making any additional deceptive privacy claims and requires that they develop and maintain a comprehensive privacy program subject to independent third-party auditors every two years for a period of twenty years.[145] While these mandatory privacy measures are likely to help ensure increased privacy protection for Facebook's users, the system is not immune from other limitations that may arise when reporting user activity that violates Facebook's service agreement. For example, attorneys Owen S. Sloan and Rachel M. Stilwell have highlighted several shortcomings in their recent article covering online impersonation laws. In one case involving a twelve-year-old victim who did not have her own Facebook account, she was faced with no alternative option but to use Facebook's online forms to report the fake profile.[146] While Facebook has since provided a way for people who do not personally have an account to report violations, their online form[147] still requires the victim to ask another person with Facebook accessibility to help them to complete questions regarding the nature of the conduct in question.

In yet another example, author Susan Arnout Smith, chronicled the difficult and lengthy weighting period she endured in order to get an imposter profile deleted after reporting the violation to Facebook.[148] A friend alerted her to the imposter profile, which contained false solicitations for sexual favors and botched photographs of Smith's head attached to a scantily clad body of another woman.[149] After several failed attempts to get the profile removed herself, Smith discovered that two students in another country were to blame.[150] She promptly contacted the school principals who were finally able to get Facebook to remove the profile after roughly one month.[151] Smith's story highlights one of the major issues with Facebook's reporting system—there is no stated time period in which Facebook is required to remove the content once it has been reported. Situations like Smith's raise important questions in determining what is reasonably expected of Facebook

---

145 Anjali C. Das, *Data Breach and Privacy Update,* WILSON ELSER (Spring 2013), http://www.wilsonelser.com/writable/files/Attorney_Articles_PDFs/databreach_privacy_2013.pdf.

146 Sloane & Stilwell, *supra* note 16.

147 *Report a Violation of the Facebook Terms,* FACEBOOK.COM (last visited Feb. 5, 2014).

148 Susan Arnout Smith, *The Fake Facebook Profile I Could Not Get Removed*, SALON.COM (Feb. 1, 2011, 8:39 PM), http://www.salon.com/2011/02/02/my_fake_facebook_profile/.

149 Sloane & Stilwell, *supra* note 16.

150 *Id*.

151 *Id*.

when a violation is reported, and further how might social media providers and government officials find alternative means to bridge their two approaches in order to resolve online impersonation cases with greater efficiency in the near future?

IV. Proposed ODR Solution

A. *Foundational Themes and Models in Online Privacy Protection*

Having highlighted critical issues barring or delaying effective litigation of online impersonation disputes, the law must innovate to provide greater protection and recourse against misuse of social media websites and other forms of electronic communication. In recent years the FTC has served as a key player in helping to identify adequate solutions to ensure greater consumer privacy online. In December 2010, roughly a year before the FTC announced its proposed settlement with Facebook, the FTC's Bureau of Consumer Protection issued a highly anticipated staff report titled, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers."[152] As stated in the report, the FTC's overarching goal in the privacy arena has been to, "protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace."[153] In working to achieve this end, the FTC has employed two specific models.[154] First, "the "notice-and-choice model," which encourages companies to develop privacy notices describing their information collection and use practices to consumers, so that consumers can make informed choices, and the "harm-based-model," which focuses on protecting consumers from specific harms—physical security, economic injury, and unwanted intrusions into their daily lives."[155] While each model has helped to achieve greater consumer privacy in the past, as im-

---

152 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers,* FTC.COM, iii (Dec. 2010) http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

153 *Id.*

154 *Id.*

155 *Id.*

plemented, a host of unforeseen limitations barring their use as long-term solutions have been identified.

> Specifically, the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand. Likewise, the harm-based model has been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored.[156]

The report further cites that these models have failed to keep pace with the rapid advancements in technology and business models, which enable companies to collect increasingly large amounts of personal data, mostly without prior consumer consent.[157] In addition, the use of self-regulatory measures such as posting privacy policies online has also proved inadequate in achieving greater privacy protection.[158] In recognizing these shortcomings, the FTC held a series of roundtable discussions from December 2009 through March 2010 with a group of key stakeholders and industry leaders to evaluate the FTC's existing approach and further develop new insights to better serve the interests of companies and consumers.[159] Several key themes that emerged from these conversations are helpful to bear in mind as guiding principles in developing a more effective resolution. These key themes provide that: (1) the collection and commercial use of consumer data is often ubiquitous and invisible to consumers, (2) consumers' lack of full information prohibits them from making informed choices online, (3) many consumers are concerned about privacy, (4) the collection and use of consumer data has led to beneficial new products and services in the market, and (5) the traditional distinction between personal identifiable information and anonymous data has blurred.[160] As a final foundational point, the FTC has historically emphasized four key elements in its online privacy work.[161] The four elements suggest that:

> (1) [B]usinesses should provide NOTICE of what information they collect from consumers and how they use it; (2) consumers should be given CHOICE about how information collected from them may be used; (3) consumers should have ACCESS to data collected about them; and (4) businesses should take reasonable

156 *Id*.
157 Federal Trade Commission, *supra* note 152.
158 *Id*. at iii, 8.
159 *Id*. at 2.
160 *Id*.
161 *Id*. at 7.

> steps to ensure the SECURITY of the information they collect from consumers. The Commission also identified ENFORCEMENT—the use of a reliable mechanism to impose sanctions for noncompliance—as a critical component of any regulatory or self-regulatory program.[162]

B. *Evaluation of Previously Proposed ODR Models*

In proposing the use of online dispute resolution (ODR) to prevent and resolve cases of online impersonation we must first define ODR as a methodology and evaluate key examples that have been implemented in related areas of law. Online dispute resolution "draws its main themes and concepts from alternative dispute resolution (ADR) processes such as negotiation, mediation, and arbitration."[163] In addition, ODR "uses the opportunities provided by the Internet not only to employ these processes in the online environment but also to enhance the processes when they are used to resolve conflicts in offline environments."[164] Historically, the Uniform Domain-Name Dispute-Resolution Policy (UDRP) "a form of non-binding online arbitration," has been widely recognized as a leading example of mass ODR.[165] In 1999, amidst rising disputes between domain name holders and trademark owners, the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation, adopted the UDRP policy to govern the resolution of domain-name and trademark disputes.[166] The primary purpose of the URDP is to "fight 'cybersquatting', that is the registration of a domain name identical to or resembling a well-known trademark with the purpose of reselling it afterwards to its owner."[167] The ICANN domain-name dispute resolution serves the primary goal of offering domain-name owners a, "quick and inexpensive online arbitration procedure to resolve disputes about domain names and hence stop the

---

162 *Id*.

163 ETHAN KATSH, JANET RIFKIN, ONLINE DISPUTE RESOLUTION 2 (2001).

164 *Id*.

165 GABRIELLE KAUFAMN-KOHLER & THOMAS SCHULTZ, ONLINE DISPUTE RESOLUTION 36 (2001).

166 *Id*. at 36–37.

167 *Id*. at 37.

action of unreasonable domain-name grabbers (also known as "cybersquatters).[168]

In the UDRP model, ICANN has accredited UDRP providers, consisting of either a sole panelist or a three-member panel, of which the complainant can choose to resolve their case.[169] Although the UDRP issues non-binding agreements in their process, the proposed model if applied to cases of online impersonation would result in a binding arbitration agreement since one of the parties would be the alleged perpetrator. The issuance of a binding arbitration agreement is, "[M]ore authoritative. They are binding in the same manner as court judgments. They are final, subject to an action to set aside, which is admissible on very limited grounds and for violation of public policy."[170] Thus, such a model achieves greater legitimacy for social media providers, transparency of procedure and resolution, government credibility and tracking and most importantly; a binding resolution for the online impersonation victim. The ICANN process has several important features: (1) when registering for a domain name, the registrant agrees to participate in an online arbitration proceeding if a complaint is filed against their domain name; (2) the arbitration agreement is not binding, permitting either party to go to court if unsatisfied with the decision; and (3) the resulting outcome is easily enforced in that the domain either remains with the registrant or is transferred to the complainant depending on who wins.[171] Thus, for purposes of this Note, the ICANN/UDRP policy serves as the prevailing model for a suggested ODR approach to resolving online impersonation disputes. Using the above as a guide the following recommendations are proposed:

Procedural and Material Components: In devising an ODR alternative it is important to consider both the procedural and material components that are essential to building a successful model. The main procedural issues taken into consideration include the appointment and independence of neutrals, confidentiality, the binding character of the outcome, duration and costs.[172] As an alternative to online impersonation statutes, social network providers like Facebook, Twitter, and LinkedIn should be encouraged to

---

168 Arno R. Lodder and John Zeleznikow, Enhanced Dispute Resolution Through the Use of Information Technology, 74 (2010).

169 Kaufamn-Kohler & Schultz, *supra* note 165 at 36.

170 *Id*. at 54.

171 *Id*. at 75.

172 *Id*. at 37.

sign cooperation agreements with state officials to devise a united ODR program.

Centralized ODR Program/Cooperation Agreements: The advantages to using a centralized online dispute resolution program as opposed to a private online ADR procedure like the system that Facebook already has in place, include greater public accountability and perceived legitimacy of the process.[173] Once these cooperation agreements are in place, social media providers and each state's cyber crime and Internet safety divisions, typically housed under the state attorney general's office, should design a uniform reporting process where all users can file violations found on the Internet or via electronic communication.

Filing Complaints Through a Unified Reporting Process: Once vetted for their legitimacy, complaints would be automatically forwarded to the social network provider where the conduct in question has taken place. By requiring users to file complaints through a centralized reporting process, state and local government officials will have greater ability to track cases and work in tandem with social media providers to promptly resolve the conflicts. Where conduct implicates further criminal behavior, state and local law enforcement will also be able to act to apprehend an identified suspect with greater efficiency should the case need to proceed to litigation. This process enables Facebook to retain control over their reporting system, but tackles the currently disjointed nature of separate reporting processes. Further, "In an environment such as [social media] which precisely lacks trust, cyber courts may thus play a useful role, supplemental to that of private ODR. They should thus be prompted not only for reasons of convenience, but because they foster confidence [in] electronic [communication]."[174]

V. CONCLUSION

E-personation, according to California Senator Simitian, "[I]s the dark side of the social networking revolution. Facebook or MySpace pages, e-mails, texting and comments on Web forums have been used to humiliate or torment people and even put them

---

173 *Id*. at 42.
174 *Id*.

in danger. Victims have needed a law they can turn to."[175] In the wake of newly enacted legislative remedies, there remain important questions that must be asked by legislatures, social media providers, and users alike. While some states such as California, New York, Texas, and Mississippi have existing online impersonation laws, others such as Arizona must not act with haste to enact remedies for their constituents without first analyzing current statutory schemes for potential deficiencies and loopholes that may arise.

The psychological motivation of those who choose to impersonate others online ranges widely from a desire to be loved and accepted to a much further extreme—a desire to obtain revenge as a result of a past wrong or personal hurt.[176] In either case, is there a difference in the particular course of action that a victim chooses to take? When the intent is to harm, the answer is—yes. The victim often faces one of two courses of action: (1) pursue costly litigation if available in their jurisdiction, or (2) place all hope for a resolution entirely in the hands of Facebook administrators. Both have strong pluses and minuses, but neither option seems to fully achieve an ideal resolution. At first glance, litigation seems like the preferred course of action in a serious case of online impersonation where the perpetrator acts with a legitimate intent to harm their victim either by posting derogatory comments or sexually explicit photographs designed to embarrass and result in public shame. In these cases, there is little hope that the perpetrator and victim will be able to talk out their differences or that the conduct will be easily resolved. In the second approach, which is more applicable to cases of online impersonation without a serious intent to harm another, as in the case of a "catfisher" who uses someone's identity to look for love, Facebook's reporting mechanisms which are entirely free, stand as a more effective option; but there is little assurance and deterrence against repeat offenses.

Current and proposed statutes are not aimed at providing effective protection against future and/or repeat cases of online impersonation. Some may argue it is too soon to judge the effectiveness of such laws. However, as cases of online impersona-

---

175 *Malicious E-Personation Protection Effective January 1,* State Senator Joe Simitian (Dec. 22, 2010), http://www.senatorsimitian.com/entry/malicious_e-personation_protection_effective_january_1/.

176 Rachel George, *Catfish Starts Share Insight into Manti Te'o Saga*, USA TODAY SPORTS (Jan. 18, 2013, 5:37 PM), http://www.usatoday.com/story/sports/ncaaf/2013/01/17/catfish-stars-nev-schulman-max-joseph-manti-teo-saga/1843155/.

tion continue to persist, the present need for an effective remedy outweighs the public's willingness to wait for state legislatures to get it right. Meanwhile, social media providers largely enjoy immunity from liability resulting from third-party generated content, yet they play a key role in helping to deter the continuance of online impersonation. At present, social media providers and state governments have attacked this ongoing problem from an entirely divided front. Moving forward, the suggestion of a URDP-based model to unite social media providers, government entities, and users will provide the benefit of increased transparency, greater cost and time efficiency, and increased assurance that users' personal information cannot be misappropriated by others without resolution. In addition, state legislatures should consider aligning future online dispute resolutions in this area of law with federal and national initiatives such as President Obama's Online Safety Technology Working Group, the National Center for Missing and Exploited Children, and Harvard University's Berkman Center for Internet & Society.