Fall 9-2014

The Challenges of Preventing and Prosecuting Social Media Crimes

Thaddeus A. Hoffmeister
University of Dayton, thoffmeister1@udayton.edu

The Challenges of Preventing and Prosecuting Social Media Crimes

Thaddeus Hoffmeister*

> Wanted: Caretaker For Farm. Simply watch over a 688 acre patch of hilly farmland and feed a few cows, you get 300 a week and a nice 2 bedroom trailer, someone older and single preferred but will consider all, relocation a must, you must have a clean record and be trustworthy—this is a permanent position, the farm is used mainly as a hunting preserve, is overrun with game, has a stocked 3 acre pond, but some beef cattle will be kept, nearest neighbor is a mile away, the place is secluded and beautiful, it will be a real get away for the right person, job of a lifetime—if you are ready to relocate please contact asap, position will not stay open.[1]

This Craigslist ad was posted in 2011 by two residents of North-Central Ohio, Brogan Rafferty (age 16 at the time) and Richard Beasley (age 52 at the time).[2] Of the four individuals (2 from within Ohio and 2 from outside of Ohio) who came to the farm to interview for this job posting, 3 were killed and robbed by Rafferty and Beasley.[3] The fourth victim was shot but managed to escape and contact authorities.[4] Both Rafferty

* Professor of Law and editor of lawandsocialmedia.wordpress.com.

1. Hanna Rosin, *Murder by Craigslist: A Serial Killer Finds a Newly Vulnerable Class of Victims: White, Working Class Men*, ATLANTIC (Aug. 14, 2013, 8:20 PM), http://www.theatlantic.com/magazine/archive/2013/09/advertisement-for-murder/309435/.

2. Thomas J. Sheeran, *Richard Beasley, 'Craigslist Killer,' Sentenced to Death*, HUFFINGTON POST (Jun. 4, 2013, 5:12 AM), http://www.huffingtonpost.com/2013/04/04/richard-beasley-craigslist-killer-death-penalty-sentence_n_3013536.html#.

3. *Id.*

4. *Id.*

and Beasley were apprehended, tried, and convicted.[5] Rafferty was sentenced to life without the possibility of parole and Beasley is currently on Ohio's Death Row.[6]

For those bent on committing crimes, like Rafferty and Beasley, social media has opened up a whole new world. It has become the place where criminal defendants not only commit crimes, but also organize, plan, discuss, and even boast about their illegal activity. Numerous criminal defendants ranging from Fortune 500 corporate officers to street level petty thieves have used social media to facilitate their criminal conduct. Social media has even garnered the attention of criminal gangs.[7] This in turn has led commentators to coin new phrases and terms like "cyberbanging."[8]

The adoption and use of social media by a broad spectrum of criminal defendants has raised some significant challenges for those tasked with crime prevention. This article will look at those challenges through the lens of three cases involving social media: *United States v. Drew*,[9] *United States v. Sayer*,[10] and *United States v. Cassidy*.[11] However, prior to beginning that examination, this article will briefly discuss and categorize the various ways criminal defendants employ social media.

I. Categorizing Criminal Activity Involving Social Media

Generally speaking, criminal defendants use social media in one of two ways. The first method by which criminal defendants employ social media involves *relaying* information to victims,[12] co-conspirators,[13] or the general public.[14] Conduct

5. *Id.*

6. *Id.*

7. Kim Russell, *Detroit Students Organize Fights Online and Then Post Videos in Practice Called Cyber-Banging*, ABC ACTION NEWS (Jan. 28, 2012, 11:37 PM), http://www.wxyz.com/news/region/detroit/detroit-public-schools-police-fighting-cyber-banging.

8. *Id.*

9. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

10. United States v. Sayer, 748 F.3d 425 (1st Cir. 2014).

11. United States v. Cassidy, 814 F. Supp. 2d 574 (D. Md. 2011).

12. *Drew*, 259 F.R.D. at 449.

13. Andrew Blankstein & Kimi Yoshino, *The Game's 'Telephone Flash Mob' Delayed Responses to Robberies,* L.A. TIMES (Aug. 13, 2011),

arising here is classified as Category I activity. This category can be further subdivided into two distinct groups (A and B). Group A consists of criminal conduct that occurs entirely online for example bullying, harassment, or stalking.[15]

Group B consists of criminal activity that occurs both online and offline.[16] The previously mentioned example from Ohio where the criminal defendants used Craigslist to lure victims to their farm and then execute them would fall into Group B.[17]

The common denominator with both groups in Category I is that the criminal defendant uses social media to *relay* information to victims, co-conspirators, or the general public. The term *relay* applies to any method by which an individual may deliver information to another via social media. This includes such things as "liking" the social media content of another user.[18] In one case from New York, a trial court determined that a defendant could be charged for violating a protection order when she sent a friend request to an individual who had a protection order against her.[19] According to the judge, the defendant's use of social media to reach the complainant was a form of contact just like speaking in person or by telephone, and the order of restraint had barred any type of contact.[20]

When relaying information to victims, co-defendants, or the general public, criminal defendants use a variety of techniques. For example, some communicate directly with the victim on social media, while others communicate indirectly by merely posting information on social media in a public or quasi-public place where the victims or the public can view it. For example, in *Griffin v. Maryland*, a case involving the authentication of a Myspace page, the girlfriend of the

http://latimesblogs.latimes.com/lanow/2011/08/game-rapper-twitter-telephone-flash-mob-sheriff.html.

14. *Sayer*, 748 F.3d at 425.

15. *Drew*, 259 F.R.D. at 449.

16. Sheeran, *supra* note 2.

17. *Id.*

18. *Tennessee Man Arrested for Facebook Like,* RT (Jan. 17, 2011), http://rt.com/usa/man-arrested-facebook-like-790/.

19. People v. Fernino, 851 N.Y.S.2d 339 (Crim. Ct. 2008).

20. *Id.*

defendant allegedly posted the following on her Myspace page as a warning to anyone who planned to testify against her boyfriend in his upcoming trial, "JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[21]

Also, when relaying information to victims, co-defendants, or the general public, some criminal defendants use their real names.[22] Others remain anonymous or create fictitious names.[23] A final group actually creates a false name or takes on the identity of the intended victim, e.g., online impersonation.[24]

The second method or category of criminal activity involves using social media to *gather* information about victims.[25] Like Category I, Category II can be further subdivided into two groups. In Group A, the criminal defendant employs the information gathered from social media to commit modern crimes that many associate with the Internet, e.g., identity theft.[26] In Group B, the criminal defendant uses information gathered from social media to commit traditional crimes such as burglary.[27]

When using social media for Category II crimes, criminal defendants look for all types of personal identifiable information about victims ranging from photos to birthdates to names of friends. According to Frank Abagnale, a former con man turned FBI officer (portrayed in the 2002 film *Catch Me If*

21. Griffin v. Maryland, 995 A.2d 791, 795 (Md. 2011).

22. United States v. Elonis, No. 11-00013, 2011 WL 5024284 (E.D. Pa. Oct. 20, 2011).

23. A.B. v. Indiana, 863 N.E.2d 1212 (Ind. Ct. App. 2007), *vacated*, 885 N.E.2d 1223 (Ind. 2008); Layshock v. Hermitage Sch. Dist., 412 F. Supp. 2d 502 (W.D. Pa. 2006).

24. Tina Susman, *Facebook Identity Theft: Probation Deal for Woman Who Trashed Ex?*, LA TIMES (Mar. 20, 2012), http://articles.latimes.com/2012/mar/20/nation/la-na-nn-fake-facebook-20120320.

25. *Facebook ID Theft Targets "Friends"*, NBC NEWS (Jan. 30, 2009), http://bob-sullivan.newsvine.com/_news/2009/01/30/2375283-facebook-id-theft-targets-friends.

26. Steve Lohr, *How Privacy Vanishes Online,* N.Y. TIMES (Mar. 16, 2010), http://www.nytimes.com/2010/03/17/technology/17privacy.html?_r=0.

27. Kim Komando, *Burglars Use Social Media to Target Homes,* USA TODAY (Jan. 3, 2014), http://www.usatoday.com/story/tech/columnist/komando/2014/01/03/social-media-identity-theft-home-videos/4248601/.

You Can), "[i]f you tell me your date of birth and where you're born [on Facebook], I'm 98% [of the way] to stealing your identity."[28]

To obtain certain personal information, criminal defendants must monitor social media over a period of time.[29] This is especially true if the criminal defendant wants to learn the physical whereabouts or daily routine of the victim.[30]

Currently, the vast majority of social media related criminal activity occurs in Category I, i.e., relaying information to others. Thus, this essay will focus on this category. It should be noted, however, that sometimes the defendant's criminal conduct falls into both Categories I and II or cuts across multiple groups.

II. *United States v. Lori Drew*

In *United States v. Lori Drew*, the defendant, a 49-year-old mother from Missouri, created a MySpace page with the picture of an attractive fictitious 16-year-old boy named Josh Evans.[31] The picture used for the MySpace page was of a real person, however, the name and information attached to the picture were entirely fake.[32] Lori Drew created this account to befriend 13-year-old Megan Meier, a one-time friend and classmate of Drew's daughter.[33] Lori Drew believed that this bogus MySpace account would allow her to learn whether Megan Meier was spreading rumors about her daughter.[34]

Acting as Josh Evans, Lori Drew would flirt with Megan

28. Mark Sweney, *Facebook Users Risk Identity Theft, Says Famous Ex-Conman*, GUARDIAN (London), (Mar. 20, 2013), http://www.theguardian.com/media/2013/mar/20/facebook-risks-identity-theft-frank-abagnale.

29. Simon Tomlinson, *How's Your Social Security? Burglars Monitor Facebook and Twitter to See When You're Away from Home,* DAILY MAIL (Nov. 1, 2011), http://www.dailymail.co.uk/sciencetech/article-2056079/Hows-social-security-Burglars-monitor-Facebook-Twitter-youre-away-home.html.

30. *Id.*

31. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).

32. *Id.*

33. *Id.*

34. *Id.*

Meier on MySpace.[35] The relationship eventually turned sour and Lori Drew, through Josh Evans, told Megan Meier that the world would be a better place without her.[36] Shortly thereafter, Megan Meier, believing she had been rejected by Josh Evans committed suicide in her closet bedroom.[37]

The federal government relying on the Computer Fraud and Abuse Act (CFAA) charged Lori Drew with three felony counts of *accessing protected computers without authorization to obtain information*.[38] At the time, the CFAA appeared to be the best federal statute to address Lori Drew's conduct. The U.S. attorney from the Central District of California handled the prosecution because the MySpace servers were physically located in California. Missouri passed on the opportunity to prosecute because at the time the state's harassment statute did not address Lori Drew's conduct.[39]

Under the government's theory of prosecution, Lori Drew violated the CFAA because she had entered into a contract or Terms of Service (TOS) agreement with MySpace in order to create Josh Evans's account.[40] Most social media providers require users to enter into a TOS established by the social media provider prior to setting up an account.[41] Pursuant to the MySpace TOS, Lori Drew was required to provide accurate and truthful information when registering for the account and *refrain from using any information obtained from MySpace services to harass, abuse, or harm other people*.[42]

Lori Drew allegedly violated this TOS when she (1) created the bogus Josh Evans account and (2) used the account to harass Megan Meier.[43] Thus, Lori Drew's communication with Megan Meier through MySpace's protected servers was without authorization or in excess of authorized access at least

35. *Id.*
36. *Id.*
37. *Id.*
38. 18 U.S.C. §1030 (2012) (emphasis added).
39. Joel Currier & David Hunn, *Neighbor's Story Emerges in Suicide; Prosecutor Finds Insufficient Evidence to Charge Anyone in MySpace Case,* ST. LOUIS POST DISPATCH, Dec. 4, 2007, at A1.
40. *Drew*, 259 F.R.D. at 464-68.
41. *Id.*
42. *Id.*
43. *Id.*

according to the prosecution.[44]

Although the jury found Lori Drew guilty, it rejected the prosecution's theory that Lori Drew intended to harm Megan Meier, a required finding for a felony conviction under the CFAA.[45] As a result, the jury only convicted Lori Drew of three misdemeanor counts.[46] These convictions were later overturned by the trial judge on vagueness grounds.[47] The trial judge determined that the CFAA as applied in the *Drew* case failed to give the defendant notice that breach of a website's TOS in and of itself could constitute a crime.[48] In addition, the judge found that such application provided insufficient guidelines to law enforcement as they attempt to enforce the law.[49]

While Lori Drew's conduct was universally condemned across the country, many felt uncomfortable with her prosecution under the CFAA.[50] The concern over the case was not necessarily for Lori Drew but what her case meant for future defendants. Had the government succeeded in its prosecution of Lori Drew, then arguably anyone could be prosecuted for violating a TOS. Thus, lying on Myspace or LinkedIn about academic or professional credentials in order to impress some reader could lead to criminal charges if the social media provider's TOS prohibited such dishonesty or fraud.

III. *United States v. Sayer*

Sayer illustrates another example of online social media impersonation; however, unlike *Drew,* the defendant here impersonated the victim (his ex-girlfriend) rather than a fictitious person.[51] In *Sayer,* the defendant posted ads on

44. *Id.*
45. *Id.* at 451.
46. *Id.*
47. *Id.* at 449.
48. *Id.* at 461.
49. *Id.* at 467.
50. Andrew M. Grossman, *The MySpace Suicide: A Case Study in Overcriminalization,* THE HERITAGE FOUND. (Sep. 17, 2008), http://www.heritage.org/research/reports/2008/09/the-myspace-suicide-a-case-study-in-overcriminalization.
51. United States v. Sayer, 748 F.3d 425, 428 (1st Cir. 2014).

Craiglist's Casual Encounters (a section on Craigslist for meeting other people) that showed his ex-girlfriend in lingerie.[52] Prior to their break-up, the defendant had taken consensual photos of the victim.[53] In the ad, Sayer, posing as his ex-girlfriend, encouraged men to come to her house.[54] The ad included the victim's address and a list of sex acts to be performed when the men arrived.[55] As a result of the ad, strange men would routinely appear at the victim's house looking for sexual encounters.[56]

In order to prevent random strangers from showing up at her house, the victim moved to Louisiana.[57] However, different men again started to arrive at her new home.[58] Like in the past, these men claimed that they had met the victim online.[59] Shortly thereafter, the victim discovered a sexually explicit video of herself on several adult pornographic sites.[60] As with the earlier pictures, the victim had consented to the video prior to her breakup with Sayer.[61] The video posting included the victim's name as well as her new Louisiana address.[62] Ultimately, Sayer was caught and successfully prosecuted for cyber stalking and identity theft.[63]

With respect to the cyber stalking charge, Sayer was convicted of violating the Federal Interstate Stalking Punishment and Prevention Act (FISPPA).[64] While the term "Facebook Stalker" has garnered a sort of benign humorous connotation in popular culture,[65] individuals, through the misuse of social media, have been charged and convicted of

52. *Id*.
53. *Id*.
54. *Id*.
55. *Id*.
56. *Id*.
57. *Id*.
58. *Id*.
59. *Id*.
60. *Id*.
61. *Id*.
62. *Id*.
63. *Id*. at 429.
64. 18 U.S.C. § 2261A (2012).
65. Byron Dubow, *Confessions of 'Facebook Stalkers'*, USA TODAY (Mar. 8, 2007), http://usatoday30.usatoday.com/tech/webguide/internetlife/2007-03-07-facebook-stalking_N.htm.

violating FISPPA. As originally written, FISPPA prohibited a person, who had crossed state lines, from using the mail or commerce to put another in reasonable fear of death or serious injury.[66] In 2000, the jurisdictional hook of the statute was changed from "travel across a State line" to "travel[] in interstate commerce."[67] This modification turned FISPPA into a statute that targeted both traditional and online stalking.[68] The law was again expanded in 2006 to criminalize causing *substantial emotional distress* to another person using an *interactive computer service*.[69] Today, for a successful prosecution under FISPPA, the government must prove the following elements:

Use of

a. The mail

b. Any interactive computer service, or

c. Any facility of interstate or foreign commerce;

To engage in a course of conduct, defined as a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose;

That causes

d. Substantial emotional distress, or

e. Reasonable fear of death or serious bodily injury, to a person in another state or tribal jurisdiction or within the special maritime and territorial jurisdiction; and

Intent by the defendant to

f. Kill,

g. Injure,

h. Harass,

66. 18 U.S.C. § 2261A Notes.
67. *Id.*
68. *Id.*
69. 18 U.S.C. § 2261A.

i. Place under surveillance with intent to kill, injure, harass, or intimidate, or
j. Cause substantial emotional distress to that person.[70]

IV. *United States v. Cassidy*

United States v. Cassidy, the last case to be discussed, highlights some of the challenges that arise with FISPPA prosecutions when the alleged stalking or harassment involves a public figure and occurs on social media. In *Cassidy*, the criminal defendant, who initially went by the alias Sanderson, met Alyce Zeoli in 2007.[71] Zeoli, an enthroned Buddhist American tulku,[72] teaches and leads the Kunzang Odsal Palyou Changchub Choling Center ("Center"), located in Maryland.[73] The meeting between Cassidy and Zeoli was facilitated by Zeoli's friends who believed that Cassidy was also a Buddhist American tulku.[74]

After meeting and becoming fast friends with Cassidy, Zeoli invited him to drive with her to a retreat in Arizona.[75] During the trip, Cassidy proposed to Zeoli but she declined his offer.[76] He then suggested that the two pretend to be married.[77] While on this trip, Zeoli also revealed intimate details about her personal life to Cassidy.[78]

Shortly after the trip, it came to light that William Sanderson's real name was William Cassidy.[79] Members of the Center also began to notice that Cassidy's conduct was inconsistent with the sect's teachings, e.g., he gossiped.[80] Yet,

70. *Id.*
71. United States v. Cassidy, 814 F. Supp. 2d 574, 578 (D. Md. 2011).
72. *Id.* (A tulku is "A reincarnate master.").
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*

despite certain misgivings, Cassidy was appointed to the position of chief operating officer (COO) of the Center.[81] Shortly after his appointment as COO, Zeoli learned that Cassidy had never been a tulku.[82] She confronted Cassidy about this fact and he left the Center in February 2008.[83]

Subsequent to his departure, Cassidy started making disparaging posts and tweets about Zeoli and the Center. Some of the 8,000 tweets and blog posts were arguably threatening:

> *ya like haiku? Here's one for ya: "Long, Limb, Sharp Saw, Hard Drop" ROFLMAO.*
> *Got a wonderful Pearl Harbor Day surprise for KPC . . . wait for it.*
> *Terrors in the night disturb Fat (A.Z.)'s sleep: she cannot sleep without taking something, and anxiety rules her body like a slavemaster.*[84]

Other tweets and posts were critical and disparaging:

> *[Zeoli] is a demonic force who tries to destroy Buddhism.*
> *(A.Z.) you are a liar & a fraud & you corrupt Buddhism by your very presence: go kill yourself.*
> *(A.Z.) IS A SATANIC CORRUPTER OF DHARMA: A SHE_DEMON WHO MASQUERADES AS A "TEACHER"*[85]

In 2011, Cassidy was charged with violating FISPPA.[86] Specifically, Cassidy was charged with the intent to *harass* and *cause substantial emotional distress* to Zeoli in violation of FISPPA.[87] Interestingly, the government did not charge the defendant with putting Zeoli in *reasonable fear of death or*

81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.* at 588.
85. *Id.* at 589.
86. *Id.* at 576.
87. *Id.*

serious bodily injury. This is most likely due to the fact that the posts and tweets, although disparaging, were not very threatening.

Prior to trial, counsel for Cassidy filed a motion to dismiss, arguing that the statute on its face and as applied violated Cassidy's First Amendment rights.[88] The trial court ultimately found the statute unconstitutional as applied to Cassidy.[89] Thus, it never decided whether the statute was unconstitutional on its face.

In dismissing the charges against Cassidy, the trial court first determined that Cassidy's tweets and blog posts, although in bad taste, challenged Zeoli's character and qualifications as a religious leader and thus were protected under the First Amendment of the United States Constitution.[90] The court pointed out that not all speech is protected, for example, speech involving obscenity, fraud, defamation, true threats, incitement, or speech integral to criminal conduct.[91] However, Cassidy was charged with harassing Zeoli, not with placing her in reasonable fear of death or serious bodily injury.

The next step in the court's analysis was to determine whether FISPPA as applied to Cassidy's actions was a content-based restriction.[92] The court ultimately determined that the statute as applied to Cassidy was a content-based restriction because it "limits speech on the basis of whether that speech is emotionally distressing to A.Z."[93]

As a result of this determination, the court examined the application of the FISPPA statute under the highest level of review—strict scrutiny.[94] Thus, in order for the government to prevail against Cassidy's motion to dismiss, it had to show a compelling interest for the prosecution of the case, a very high standard to meet.

The government claimed that its compelling interest arose from the need to protect "victims from emotional distress

88. *Id.* at 581.
89. *Id.* at 587.
90. *Id.* at 583.
91. *Id.*
92. *Id.*
93. *Id.* at 584.
94. *Id.*

sustained through an interactive computer service."[95] The court pointed out, however, that this interest could just as easily be protected by having the victim ignore the defendant's blog or block his tweets.[96]

The court then went on to examine whether the government could survive the defendant's motion to suppress under a lower level of review—intermediate scrutiny.[97] Unfortunately for the prosecution, the court again found the government's argument for prosecuting Cassidy under FISPPA unconstitutional even with this lower level of scrutiny.[98] Here, the court drew a distinction between using the telephone to harass someone and using Twitter or a blog.[99] In explaining why Virginia's telephone harassment statute could be found constitutional while FISPPA as applied to Cassidy could not, the court stated, "harassing telephone calls 'are targeted towards a particular victim and are received outside a public forum'. . . Twitter and Blogs are today's equivalent of a bulletin board that one is free to disregard, in contrast, for example, to e-mails or phone calls directed to a victim."[100]

The court's opinion did not end with finding the government's interest to be lacking at both levels of scrutiny. The court went on and assumed *in arguendo* that the government had a compelling interest.[101] The court still found the indictment as applied to Cassidy unconstitutional because FISPPA, in this case, "sweeps in the type of expression that the Supreme Court has consistently tried to protect."[102] For example, the statute could cover statements Cassidy made about "KPC's beliefs and A.Z.'s qualifications as a leader."[103]

Cassidy might have resulted in a better outcome for the government if the defendant, rather than using social media, had employed traditional communication methods like the mail

95. *Id.*
96. *Id.* at 585.
97. *Id.*
98. *Id.* at 587.
99. *Id.*
100. *Id.* at 585.
101. *Id.* at 586
102. *Id.*
103. *Id.*

or the telephone. The court appeared troubled with prosecuting someone for making disparaging comments about a public figure in a public forum. The court noted "that Twitter and Blogs are today's equivalent of a bulletin board that one is free to disregard, in contrast, for example, to e-mails or phone calls directed at the victim."[104] The court went on to find that a blog is similar to a cyberspace bulletin board.[105]

The government also might have survived the defendant's motion to dismiss by changing its theory of prosecution from causing emotional distress to issuing true threats.[106] As the court pointed out, true threats like obscenity, fraud, incitement, and speech integral to criminal conduct are not protected speech;[107] however, that was not the basis for the government's indictment in this case. According to the court, "the Government did not seek an Indictment on the basis that the Defendant intentionally used the Internet to put A.Z. in reasonable fear of death or serious bodily injury."[108]

V. Challenges of Preventing and Prosecuting Social Media Crimes

At present, many think that social media crimes are easier to commit and more difficult to prevent than their offline counterparts.[109] For example, in the past, a crime like harassment generally required a criminal defendant to interact physically or telephonically with the victim. Furthermore, criminal defendants were historically constrained by the volume of their voices and the physical proximity of the victim. Harrasers in the Digital Age do not face these same type of impediments.

As illustrated by *Sayer*, harassment can now occur without the criminal defendant ever speaking to or interacting with the

104. *Id.* at 585-86.
105. *Id.*
106. *Id.* at 583.
107. *Id.*
108. *Id.* at n.11.
109. Jacqueline D. Lipton, *Combatting Cyber-Victimization,* 26 BERKELEY TECH L.J. 1103 (2011).

victim.[110] In fact, the criminal defendant does not even need to leave his house to commit the crime. Nor does it matter if the victim moves away because he or she can be easily tracked down by their Digital Footprint.[111] Also, with social media the criminal defendant can harass the victim through third parties who may or may not know that they are part of a criminal enterprise.

The next section will examine some of the major challenges that arise when attempting to prevent and prosecute social media related criminal activity. Specifically, this section will focus on the (1) reach of social media; (2) identification of social media users; and (3) applicable criminal statutes.

A. *Reach of Social Media*

With social media and its expansive reach (Facebook alone has over 1.2 billion users),[112] the pool of potential victims for criminal defendants has grown exponentially. In the example of the so-called Ohio "Craigslist Killers" the criminal defendants were able to go beyond their own immediate physical surroundings and find victims both inside and outside of the state.[113] One victim travelled all the way from South Carolina in response to the job advertisement.[114] By victimizing individuals from various areas of the country, the defendants reduced the likelihood that the victims would be traced back to them or that their scheme would be uncovered. The reach of social media was also seen in *Sayer* where, despite moving far away, the victim was still being harassed by her ex-

110. United States v. Sayer, 748 F.3d 425 (1st Cir. 2014).

111. *Cf.* Thaddeus Hoffmeister, *Investigating Jurors in the Digital Age: One Click at a Time,* 60 KAN. L. REV. 611, 627 (2012).

112. Jemima Kiss, *Facebook's 10th Birthday: From College Dorm to 1.23 Billion Users,* GUARDIAN (London) (Feb. 3, 2014), http://www.theguardian.com/technology/2014/feb/04/facebook-10-years-mark-zuckerberg.

113. Hanna Rosin, *Murder by Craigslist: A Serial Killer Finds a Newly Vulnerable Class of Victims: White, Working Class Men*, ATLANTIC (Aug. 14, 2013, 8:20 PM), http://www.theatlantic.com/magazine/archive/2013/09/advertisement-for-murder/309435/.

114. *Id.*

boyfriend.[115]

Since criminal defendants can easily reach victims via social media, they are more inclined to repeat their crimes. In *Sayer,* the criminal defendant used Craigslist's Casual Encounters site to re-victimize his ex-girlfriend.[116] The criminal defendant in *Cassidy* made over 8,000 disparaging blog posts and tweets about Alyce Zeoli and the Center.[117] With social media, criminal defendants can harm victims rapidly and repeatedly.

B. *Identification of Social Media Users*

One of the biggest challenges with preventing and prosecuting social media related crimes is identification of users. This is true both for victims and law enforcement. To date, neither social media providers nor the government has established a cost-effective method to verify social media users. Furthermore, it is not entirely clear that society wants either the government or social media providers to have this ability. As a result, it is not difficult for criminal defendants to remain anonymous or impersonate others on social media. Last year, Facebook reported that 7–8 percent of its accounts or approximately 50 million were fictitious.[118]

In *Drew,* Megan Meier did not know that she was communicating with a middle-aged woman and in *Sayer* the men visiting Sayer's ex-girlfriend were unaware of the fact that it was actually Sayer posting the ads. This all raises an interesting question of why impersonation works so well on social media. It appears that the success of online impersonation hinges on social media's ability to replicate human interaction. Unlike traditional forms of communication such as the mail, telephone, or television, social media comes very close to approximating face-to-face contact. This in turn

115. *Sayer*, 748 F.3d at 428.

116. *Id.*

117. United States v. Cassidy, 814 F. Supp. 2d 574 (D. Md. 2011).

118. Jim Edwards, *Facebook Targets 76 Million Fake Users in War on Bogus Accounts*, BUSINESS INSIDER (Mar. 5, 2013, 4:38 PM), http://www.businessinsider.com/facebook-targets-76-million-fake-users-in-war-on-bogus-accounts-2013-12.

leads users to believe that the individual at the other end of the laptop, tablet, or smartphone is who she says she is.

Another reason online impersonations are successful is that social media has reshaped the nature of relationships. This started with re-defining the word "friend." With social media, users create friendships online with people that they do not really know in the traditional sense; that is, most people who use social media have not interacted with (beyond accepting a friend request) or physically met all of their online friends. This in turn leads to a breakdown of the traditional social barriers that kept strangers apart. This reshaping of human interaction has progressed to the point where individuals have "dating" relationships completely online. While this is more common with Digital Natives,[119] see e.g., Mant'i Teo,[120] it is not unheard of with Digital Immigrants.[121] In fact, there was even a documentary film (Catfish) dedicated to exploring these relationships.[122]

C. *Applicable Criminal Statutes*

The third major challenge to combatting social media related crime concerns the availability of applicable criminal statutes. In certain instances, legislators have failed to keep pace with technological advancements. For instance, while identity theft is a recognized crime in every state,[123] the same cannot be said for online impersonation.[124] Unlike identity theft, online impersonation, generally speaking, lacks an economic component. Instead, the criminal defendant impersonates an individual for a noneconomic reason such as

119. Those born with the Internet.

120. Erik Brady & Rachel George, *Manti Te'o's "Catfish" Story Is a Common One,* USA TODAY (Jan. 18, 2013), http://www.usatoday.com/story/sports/ncaaf/2013/01/17/manti-teos-catfish-story-common/1566438/.

121. Those who immigrated to the Internet.

122. CATFISH (MTV Networks 2014).

123. Susan Brenner & Megan Rehberg, *"Kiddie Crime"? The Utility of Criminal Law in Controlling Cyberbullying,* 8 FIRST AMEND. L. REV. 1, 73 (2009).

124. WYO. STAT. ANN. §6-3-902 (West 2011); S. 4014, 2011, 235 Sess. (NY 2012).

to harass.[125] To date, few states have passed laws directly targeting online impersonation.[126]

In other instances, there is a law in place but it is not directly on point. This in turn leads some prosecutors to get creative which, can make the problem worse. The *Drew* case serves as a shining example.

In *Drew,* the state of Missouri declined to prosecute Lori Drew because the Missouri criminal harassment statute did not cover her specific conduct.[127] Missouri's harassment statute has been modified since then.[128] Missouri's inaction led the federal government to action. However, like the state of Missouri, the federal government did not have a law that directly addressed Lori Drew's conduct. This in turn led them to try and shoehorn the facts of the *Drew* case into the CFAA,[129] which created a backlash as many then saw Drew's prosecution as an encroachment on the constitutional rights of society as a whole.[130]

Finally, there are instances where there is an available and appropriate law in place, but when applied to social media rather than traditional forms of communication it is deemed unconstitutional. This is what occurred in *Cassidy* where the court dismissed the government's indictment, finding that it infringed on the criminal defendant's First Amendment rights.[131] A key issue in *Cassidy* was the method used by the defendant to communicate his views.[132] The court made note of the fact that rather than use the phone or email to make disparaging comments directly to the victim, the defendant used public forums such as Twitter and blog posts.[133] The court

125. SUSAN BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 87 (2010).

126. Notable exceptions include California, Connecticut, Hawaii, Mississippi, New York, Texas, Washington, and Wyoming. *See* CAL. PENAL CODE §528.5 (West 2011); MISS. CODE ANN. §97-45-33 (West 2011); TEX. PENAL CODE ANN. §33.07 (West 2011); WASH. REV. CODE §4.24.790 (West 2012).

127. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

128. MO. ANN. STAT. §565.090 (West 2013).

129. *Drew*, 259 F.R.D. at 449.

130. Grossman, *supra* note 50.

131. United States v. Cassidy, 814 F. Supp. 2d 574 (D. Md. 2011).

132. *Id*. at 576.

133. *Id*.

went on to compare these social media platforms to bulletin boards that the victim had the option of reading.[134] The court was extremely concerned about prohibiting private individuals from using social media to criticize and disparage others, especially public figures.[135]

One take away from *Cassidy* is that prosecutors and legislators will have a more difficult time preventing harassment via a public forum like Twitter or a blog post as opposed to harassment via a telephone call, letter, or email. Put differently, one-to-many speech, which generally encompasses social media, is going to face tougher constitutional scrutiny than one-to-one speech like a telephone call, letter, or email.

Due to time and space limitations, this article cannot offer a complete analysis of all the challenges facing those tasked with preventing and prosecuting social media related criminal activity. However, that was not the purpose of the article. Instead, the intent was merely to offer a brief snapshot of some of the major concerns that have arisen in this area of law.

As the cases and prior discussion demonstrate, stopping social media related crimes is no easy task. In fact, it appears, at present, that criminal defendants have the upper hand. Fortunately, this advantage will most likely be short-lived. This is because law enforcement has been steadily adapting to the Digital Age and incorporating social media into every aspect of policing. For example, agencies from the New York City Police Department to the Florida Fish and Wildlife Conservation Commission have established their very own social media units or dedicated personnel to investigate and monitor social media.[136]

Furthermore, legislators and prosecutors are now taking proactive steps to prevent criminal defendants from exploiting social media for criminal purposes. By way of example, several

134. *Id*.

135. *Id*. at 581.

136. Leslie Horn, *NYPD Social Media Unit Goes After Criminals Online*, PC (Aug. 10, 2011, 6:05 PM), http://www.pcmag.com/article2/0,2817,2390857,00.asp; *See* JOHN BROWNING, A LAWYER'S GUIDE TO SOCIAL NETWORKING: UNDERSTANDING SOCIAL MEDIA'S IMPACT ON THE LAW (Eddie Fournier ed., 2010).

states have passed laws banning certain criminal defendants from social media.[137] Also, many prosecutors are now routinely using social media in their cases. According to one Los Angeles district attorney, "the first thing I do when I get a case is to Google the victim, the suspect, and all the material witnesses. I run them all through Facebook, Myspace, Twitter, YouTube and see what I might get."[138]

137. Jonathon Hitz, *Removing Disfavored Faces from Facebook: The Freedom of Speech Implications of Banning Sex Offenders from Facebook,* 89 IND. L.J. 1327 (2014).

138. Robin Sax, *Watch What You Say . . . Online*, HUFFINGTON POST (July 19, 2009, 5:12 AM), http://www.huffingtonpost.com/robin-sax/watch-what-you-say-online_b_217366.html.