What's the Difference Between Private and Public on Social Media? A Push for Clearer Language in the Illinois Cyberstalking Statute

Gina Leahy

Follow this and additional works at: https://via.library.depaul.edu/law-review

Part of the Law Commons

Recommended Citation
Available at: https://via.library.depaul.edu/law-review/vol66/iss3/5
WHAT'S THE DIFFERENCE BETWEEN PRIVATE AND PUBLIC ON SOCIAL MEDIA? A PUSH FOR CLEARER LANGUAGE IN THE ILLINOIS CYBERSTALKING STATUTE

INTRODUCTION

It is no secret that anything one puts on social media becomes infinitely available.\(^1\) Many social media outlets’ terms and conditions, like those of Facebook,\(^2\) explicitly outline that these organizations have the right to share any and all information that is posted on their websites.\(^3\) Despite these enumerated terms and conditions, most social media users have some expectation of privacy regarding what they post on their personal accounts.\(^4\) For example, the Facebook “friend” option allows users to pick and choose with whom they want to share information.\(^5\) Nevertheless, courts across the country have held that “private” social media posts can be used as evidence in both civil and criminal trials.\(^6\) In fact, the Third Party Doctrine explicitly mandates

---

1. *RPT-Obama Warns U.S. Teens of Perils of Facebook*, REUTERS (Sept. 8, 2009, 4:55 PM), http://www.reuters.com/article/idUSN0828582220090908 (“I want everybody here to be careful about what you post on Facebook, because in the YouTube age, whatever you do, it will be pulled up again later somewhere in your life.”).
4. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1141 (2009) (“Not everything posted on Facebook is public. Users shouldn’t automatically lose their rights of privacy in information solely because it’s been put on Facebook somewhere.”).
6. Largent v. Reed, No. 2009-1823, 2011 Pa. Dist. & Cnty. Dec. LEXIS 612, at *12–13 (Pa. C.P. Franklin Cty. Nov. 8, 2011) (“The Court holds that no general privacy privilege protects [defendant’s] Facebook material from discovery. No court has recognized such privilege, and neither will we. By definition, there can be little privacy on a social networking website.”). Even if plaintiff used privacy settings that allowed only his “friends” on Facebook to see postings, he “had no justifiable expectation that his ‘friends’ would keep his profile private.” United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012). In fact, “the wider his circle of ‘friends,’ the more likely his posts would be viewed by someone he never expected to see them.” *Id.*
these social media organizations divulge their content to any third-party involved in litigation.7

This Comment argues that the Illinois legislature should amend the Cyberstalking Statute8 (the Statute) to ensure defendants are put on notice of the possible violations and consequences of their own personal acts directed towards the victim on social media platforms, and to ensure that victims are thoroughly protected from those harmful actions. Specifically, the legislature needs to provide language in the Statute that addresses the legal ramifications of posting material, directed toward the victim, on social media platforms. Nowhere in the current Statute does the phrase “social media” appear.9 This Comment argues that Illinois' stalking law, as it is currently written, does not adequately inform defendants of the statutory social media restrictions. This lack of information creates problems for potential violators and does not protect victims. The law in its current form is unclear as to which types of social media communication constitute a violation of the “contact” or “stalking” elements of the Statute.10 To correct this problem, the Illinois General Assembly should clear up the misconceptions by adding a mens rea element to the Statute.

To understand why the Illinois General Assembly should amend the current Statute, it is important to understand the background and purpose of the Statute itself. According to the U.S. Department of Justice, in 2006, an estimated 3.4 million people were stalked in the United States.11 Part II of this Comment discusses current stalking legislation in Illinois and introduces the topic of cyberstalking.12 It also gives insight as to how courts across the country interpret the term “contact” in stalking statutes. Part III analyzes different portions of the Statute and discusses Illinois v. Relerford,13 the first Illinois Appellate Court case to declare a portion of the Illinois Cyberstalking Statute unconstitutional.14 Finally, Part IV explains the

---

7. See infra notes 234–45 and accompanying text.
9. See id.
10. See id.
12. See infra notes 16–151 and accompanying text.
13. 56 N.E.3d 489.
14. See infra notes 152–276 and accompanying text.
2017] ILLINOIS CYBERSTALKING STATUTE 903

impact that the implementation of a social media and mens rea component to the Statute will have on future litigation.15

This Comment proposes a balance between instituting a clear social media and mens rea component into the Statute while protecting the due process and freedom of speech rights of defendants.

II. BACKGROUND

Stalking is a form of unwanted harassment that causes a “reasonable person” to feel fear.16 Stalking can include unwanted contact via “phone, mail, and/or email.”17 It can also include following or waiting for the victim, making direct or indirect threats to harm the victim, damaging the victim’s property, or harassing the victim through electronic communication.18 Stalking can cause permanent physiological and emotional damage and may also involve severe, sometimes lethal, violence.19

Stalking is a form of domestic abuse that has become a widespread problem.20 Batterers use stalking as a means of controlling their intimate partners.21 Stalking commonly begins during a relationship, as opposed to at its end.22 Stalking is a very serious crime,23 for which plenty of legislation criminalizing the conduct already exists.24

15. See infra notes 277–318 and accompanying text.
17. Id.
18. Id.
21. See Elizabeth M. Schneider, Battered Women and Feminist Lawmaking, 23 WOMEN’S RTS. L. REP., 243, 244 (2002). Literature discussing stalking lends support to this proposition. See Heather C. Melton, Stalking in the Context of Intimate Partner Abuse: In the Victim’s Words, 2 FEMINIST CRIMINOLOGY 347, 361 (2007). Another leading study on stalking explained, “The stalking partners’ control and dominance over women’s thinking and actions alienated them from their own goals, intentions, thoughts, feelings, and it isolated them from others.” TK LOGAN ET AL., PARTNER STALKING: HOW WOMEN RESPOND, COPE, AND SURVIVE 135 (2006).
22. LOGAN ET AL., supra note 21 at 135.

Victims experience fear for their safety, fear for the safety of others and suffer emotional distress. Many victims alter their daily routines to avoid the persons who are stalking them. Some victims are in such fear that they relocate to another city, town or state. While estimates suggest that 70% of victims know the individuals stalking them, only 30% of victims have dated or been in intimate relationships with their stalkers.

Id.

A more modern form of stalking is cyberstalking—essentially stalking performed online—which comes in all different forms. Cyberstalkers use email, messenger applications, and social media platforms to stalk their victims.

Celebrities have increasingly become the victims of cyberstalking. By viewing celebrity posts, celebrity stalkers feel like they have developed a relationship with the celebrity. In fact, many of these stalkers believe the celebrities are talking directly to them. For example, in 2012, famous model Kourtney Reppert was the victim of Facebook stalking. Luis Plascencia stalked Reppert by sending her threatening and harassing messages through email and Facebook.

25. Karen McVeigh, “Cyberstalking ‘Now More Common’ than Face-to-Face Stalking,” GUARDIAN (Apr. 8, 2011, 1:31 PM), https://www.theguardian.com/uk/2011/apr/08/cyberstalking-study-victims-men (“Cyberstalking is now more common than physical harassment, according to new figures due to be released next week, with many victims finding themselves pursued by complete strangers online.”).

26. Marian Merritt, Straight Talk About Cyberstalking, NORTON, http://us.norton.com/cyberstalking/article (last visited Mar. 8, 2017) (“It has been defined as the use of technology, particularly the Internet, to harass someone. Common characteristics include false accusations, monitoring, threats, identity theft, and data destruction or manipulation. Cyberstalking also includes exploitation of minors, be it sexual or otherwise.”).

27. Id. (“The harassment can take on many forms, but the common denominator is that it’s unwanted, often obsessive, and usually illegal.”).


30. Alexandra Katehakis, Cyberstalking: Fastest Growing Crime, HUFFINGTON POST (May 6, 2015), http://www.huffingtonpost.com/alexandra-katehakis-mft/cyberstalking-fasting-growing-crime_b_6810154.html (“Where some of us may poke our nose into Facebook a little too often, or fanatically follow a celebrity online, a cyberstalker will go further by repeatedly sending unwanted anonymous messages, threats or comments, and will continue doing these things despite repeated requests and warnings to stop.”).

31. See Kovacik & Simone, supra note 29.

32. Id.

33. Id.; see Internet Fame Draws Cyberstalker for Model Kourtney Reppert, Others, FOX NEWS (July 10, 2012), http://www.foxnews.com/entertainment/2012/07/10/internet-fame-draws-cyberstalker-for-model-kourtney-reppert-others/ (“‘I’m going to stab you in the f—— heart and cut your f—— head off. I will kill your parents, cut them to pieces with a handsaw, do you f—— understand me? Don’t f—— with me or make me mad,’ one email from her stalker allegedly read.” (alterations in original)).
In addition to celebrities being stalked on Facebook, many ex-lovers have resorted to social media in an effort to monitor old flames. A man from Maryland was convicted of stalking his ex-wife for setting up fake online profiles in her name. The man set up fake profiles on websites like Facebook and Craigslist, claiming to be his ex-wife. He then told a man to come to her house and rape her. Both instances exemplify why it is important that the legislature implement strict cyberstalking laws to ensure that victims of online abuse are protected.

A. Stalking Legislation in the United States

The legal definition of stalking varies among jurisdictions. In some states, there must be an element of victim fear and emotional distress; other states require a specific intent of the stalker. Moreover, some state laws specify that the victim must have been frightened by the stalking, but other states only require that the stalking would have caused a reasonable person to experience fear. Although Cyberstalking legislation has increased throughout the years, it is clear that each state has its own inconsistent idea of how to combat the problem.

B. Stalking Legislation in Illinois

Illinois’ stalking legislation has proven to be one of the strictest stalking statutes developed in the nation. In Illinois, stalking occurs

34. See “Friending an Old Flame on Social Media, FOCUS FAMILY (Sept. 30, 2016, 4:25 PM), http://family.custhelp.com/app/answers/detail/a_id/26281/

35. Amber Ferguson, Md. Man Convicted of Cyberstalking His Ex-Wife, NBC4 WASH. (June 13, 2013, 6:26 PM), http://www.nbcwashington.com/news/local/Md-Man-Convicted-of-73-Counts-of-Cyberstalking-Stalking-Ex-Wife-211445501.html (“The jury convicted Johnson after deliberating for three hours. He was found guilty of one count of stalking, 10 counts of reckless endangerment, two counts of harassment, seven counts of harassment by electronic mail and 53 counts of violation of a protective order.”).

36. Id. (“Johnson also set up fake online profiles, claiming to be her, on Facebook, Craigslist, Blackplanet and other Internet sites, asking men to come to her house for sex and, in one posting, telling men to come to her house and rape her.”).

37. Id.


39. See, e.g., CAL. PENAL CODE § 646.9 (West 2008); FLA. STAT. § 784.048 (2016); TENN. CODE ANN. § 39-17-315 (2016).

40. See generally CATALANO, supra note 38.

41. See, e.g., D.C. CODE § 22-3133 (2016).

42. See, e.g., GA. CODE § 16-5-90 (2013).

when a person knowingly engages in conduct that is directed at a specific target and “knows (or should know) that these actions would cause a reasonable person to fear for his/her safety, fear for the safety of another person, or suffer emotional distress.” There are two elements to stalking: (1) “following or placing [the victim] under surveillance and (2) at any time threatening [the victim] with or placing [her] in reasonable apprehension of bodily harm, sexual assault, confinement, or restraint.” Both of these elements must be met to bring a stalking charge against the alleged abuser. Stalking behavior could include following, monitoring, observing, conducting surveillance, or threatening the victim. A relatively new crime that has been broadly defined is Cyberstalking. Because the internet is somewhat low cost, easy to use, and anonymous in nature, it sets itself up to be an “attractive medium” for scams, child exploitation, and online stalking. In addition, because it is new, many states have struggled to adequately implement cyberstalking statutes.

C. Cyberstalking

With advancements in technology, stalkers are finding new ways to gather information about their victims through the use of the Internet.

46. Id.
47. Stalking No Contact Orders, supra note 44. Other examples of contact could include any of the following actions that a person directs towards you:
   - being in your physical presence; appearing within your sight; approaching or confronting you in a public place or on private property; appearing at your workplace or home; entering onto or remaining on property that you own or lease or are currently occupying; placing an object on, or delivering an object to, property owned, leased, or occupied by you.
   As technology evolves, so does the practice of cyberstalking. A web-savvy stalker can wreak havoc on the life of a victim, both online and offline. This can be incredibly damaging, particularly as more people use the Internet to pay bills, make friends, date, work, share ideas and find jobs.
50. See Online Harassment & Cyberstalking, supra note 48. (“All states have anti-stalking laws, but the legal definitions vary. Some state laws require that the perpetrator, to qualify as a stalker, make a credible threat of violence against the victim. Others require only that the stalker’s conduct constitute an implied threat.”).
ternet. Legislation addressing the issue of cyberstalking must be adaptive and constantly updated to ensure that victims are protected. Cyberstalking is hard to legally address because the stalker could be “in another state or sitting three cubicles away from the victim.” Victims and law enforcement agencies may have trouble confirming the stalker’s identity because the Internet provides a great degree of anonymity. Relatively few federal statutes address cyberstalking. The federal government appears to have left it up to the individual states to determine what constitutes cyberstalking. In turn, nearly every state has enacted legislation that targets cyberstalking.

It is very easy for abusers to stalk their victims online. Many cyberstalkers use online forums and social networking sites such as Twitter, Facebook, and Myspace. Cyberstalkers tend to conduct personal research on individuals by requesting their victims as friends on social media sites while disguising their true identity with that of someone else. Many cyberstalkers then post defamatory statements about their victim on the internet to get a reaction from the victim, and thus initiate contact.

51. Id.
53. See Online Harassment & Cyberstalking, supra note 48.
54. Id. (“In the anonymous world of the Internet, it is difficult to verify a stalker’s identity, collect the necessary evidence for an arrest and then trace the cyberstalker to a physical location.”).
56. Id.
58. Dan Tynan, Online Stalking Made Easy, PCWORLD.COM (Jan. 26, 2009, 2:15 PM), http://www.pcworld.com/article/158347/online_stalking_spokeo.html (“In other words, for just $3 to $5 a month Spokeo gives you the ability to stalk near-total strangers in new and fascinating ways.”).
59. See McVeigh, supra note 25.
60. Id.
61. Id.
Cyberstalkers vary in age. In 2011, a twelve-year-old girl from Washington was convicted of cyberstalking and computer trespass in the first degree. On March 18, 2011, the girl hacked her former friends Facebook page. She posted threatening images targeting the victim. The girl then sent out messages to the victim’s Facebook friends asking for sexual favors. Another example occurred in 2013 when a family was sentenced to life in prison for the first federal cyberstalking conviction in the United States. The defendants included a mother, brother, and sister. The family used mail, email, websites and internet postings to disseminate false allegations that the brother’s ex-wife had abused her children and suffered from mental illness. On February 11, 2013, the father murdered his ex-daughter-in-law in a courthouse, before killing himself. The prosecutor in the case argued that the murder was “reasonably foreseeable” to the family’s cyberstalking. A federal jury convicted the mother, brother, and sister of interstate stalking and cyberstalking, and found each individual criminally responsible for the ex-wife’s death.

D. Cyberstalking in Illinois

Illinois has taken numerous steps to ensure that victims of cyberstalking are protected. In 2001, the Illinois General Assembly enacted the Cyberstalking Statute that dealt specifically with electronic communication. In January 2010, the Illinois General Assembly en-

63. Id. ("The 12-year-old . . . was sentenced to six months of probation and 20 hours of community service, along with mandatory adult supervision of all computer usage.").
64. Id.
65. Id.
66. Id.
68. Id.
69. Id.
70. Id.
71. Id.
72. Id.
73. Cyberstalking, 720 ILL. COMP. STAT. 5/12-7.5 (2014), invalidated in part by Illinois v. Relerford, 56 N.E.3d 489 (Ill. App. Ct. 2016) (holding that subsections (a)(1)–(2) were facially unconstitutional under the Due Process Clause of the Fourteenth Amendment because they lacked a mens rea requirement).
acted the Stalking No Contact Order Act (No Contact Act).\footnote{75} The No Contact Act gave victims who have not had a dating or intimate relationship with their stalker an opportunity to have their concerns addressed in a court proceeding.\footnote{76} In Illinois, if an individual feels that she is being stalked, she can file for a Stalking No Contact Order.\footnote{77} “A petition for a stalking no contact order can be filed in the county where [the victim] live[s], where the stalker lives, or where one or more acts of stalking took place.”\footnote{78} In order to obtain a Stalking No Contact Order, the victim must show a pattern of stalking behavior on behalf of the respondent.\footnote{79} This pattern of behavior, or course of conduct, must consist of at least two acts of stalking behavior.\footnote{80} The conduct can be direct or indirect.\footnote{81} The Stalking No Contact Order is a civil remedy.\footnote{82} Therefore, once a respondent violates the order, there is a hearing in a civil courtroom.\footnote{83}

E. Violating the Stalking No Contact Order

In Illinois, a violation of any civil Stalking No Contact Order, whether issued in a civil or criminal proceeding, has the potential to become a criminal charge.\footnote{84} Criminal orders of protection and civil orders are inherently different.\footnote{85} Criminal orders are issued simultaneously upon domestic violence arrests.\footnote{86} On the other hand, to obtain a civil order, the victim must appear before either civil or family court to petition that court for a protection order.\footnote{87} Another important difference is how the respondent is served with the order.\footnote{88} In a criminal case, the respondent is usually served at the arraignment, while in front of the judge.\footnote{89} For a civil order, the victim is responsi-
ble for sending notice to the respondent and a preliminary hearing occurs before a judge to decide if the order should be put in place.90

The No Contact Act lists various definitions of “contact” that are prohibited.91 “Contact” under the Not Contact Act includes, “any contact with the victim, that is initiated or continued without the victim’s consent, or that is in disregard of the victim’s expressed desire that the contact be avoided or discontinued.”92 If the respondent has “contacted” the victim more than once he has opened himself up to a possible order being issued against him.93

F. Courts’ Interpretation of Contact

Courts across the country have interpreted the word “contact” very broadly. Some courts have interpreted “contact” to include posting messages on a personal Facebook page that in some way, shape, or form, addresses the victim.94 For example, in New Hampshire v. Craig,95 the New Hampshire Supreme Court interpreted “contact” to include posting messages on social media.96 The court found that posting on a social media site constituted contacting the victim and therefore was a violation of the restraining order.97 Notably, the victim in this case was not a “friend” of the defendant on Facebook.98 Rather, the victim’s mother informed the victim of what was on the defendant’s Facebook page and the victim subsequently went to search for the post.99 Nevertheless, the court ultimately concluded

90. 740 ILL. COMP. STAT. 21/60 (2014).
91. Id. § 10.
92. Id.
93. Id.
95. Id. at 559.
96. Id. at 566.
97. Id.
98. Id. at 563.
99. Id.
that the defendant’s personal Facebook page constituted a public forum.100

In Craig, the defendant was convicted of criminal threatening, witness tampering, and stalking.101 The convictions were based on messages that he posted on his Facebook profile page directed to the victim.102 The defendant followed the victim to her workplace, where “their relationship consisted only of ‘very casual, very simple’ customer-server communications.”103 The defendant then started sending the victim letters addressed to her work.104 The victim received a restraining order against the defendant.105 “The restraining order required the ‘[s]toppage of the mail letters and no contact whatsoever, phone, email, et cetera.’”106 After being served the order, the defendant continued to post about the victim on his page.107 Part of the post stated, “HA HA. I mentioned Facebook in a letter, you mentioned your knowledge of it in your complaint, yet did not say not to talk about you on here.”108 The victim accessed the defendant’s Facebook page and saw the post.109 “Although the victim had a Facebook page at the time, she was not a ‘Facebook friend’ of the defendant.”110

After being convicted of stalking the victim, the defendant appealed his case.111 On appeal, he argued that “there was insufficient evidence that he stalked the victim because he did not take an ‘action to communicate’ with the victim as required by the definition of ‘contact’” in the relevant stalking statute.112 The defendant contended that in order for his conduct to constitute “contact” pursuant to the stalking statute, he must have been “the actor not only in the creation of the message, but in the conveyance of it to the protected person.”113 The defendant further argued that his Facebook posts could not constitute contact because he did not send the posts directly to the victim.114

100. Craig, 112 A.3d at 566.
101. Id. at 560, 563.
102. Id. at 561.
103. Id.
104. Id.
105. Id.
106. Craig, 112 A.3d at 561.
107. Id.
108. Id. at 562.
109. Id. at 563.
110. Id.
111. Id.
112. Craig, 112 A.3d at 565.
113. Id. at 566.
114. Id. (“[H]e merely posted publicly online without sending the posts directly to the victim, and, therefore, did not take an ‘action to communicate’ as required by [the statute].”).
The court ultimately held that the defendant’s post did constitute contact. The court reasoned that the statute only requires that a person act “either directly or indirectly” to “communicate with another.” The court further explained that the stalking statute was meant to be construed liberally and that the purpose of the statute was to “preserve and protect the safety of the family unit for all family or household members by entitling victims of domestic violence to immediate and effective police protection and judicial relief.”

Another case considering contact via Facebook is O’Leary v. Florida. In O’Leary, the defendant filed an appeal for the denial of his motion to dismiss two counts of sending written threats to kill or do bodily harm in violation of a Florida statute. The defendant posted a statement on his personal Facebook page which “threatened death or serious bodily injury” to his relative. The defendant’s cousin, who was not the target of the statement, was friends with the defendant on Facebook and therefore able to view the statement. The parties did not dispute that the defendant never expressly asked his cousin to view the Facebook page or the threatening post. Nevertheless, the cousin viewed the post. The cousin then showed the threatening post to his uncle, and the uncle told the victim about the defendant’s post.

The defendant argued that, by posting his message on his personal Facebook page, he “at most, published the message, which is not a violation of the statute.” He further argued that he “sent” nothing because he never asked anyone to look at the page. The court in O’Leary relied on Florida v. Wise, which dealt with a defendant that was sending threatening letters to a victim while he was in jail. The court in Wise created a two-part test to determine what constitutes “sending” a message for the purposes of the Florida threatening

---

115. Id. at 569.
116. Id.
117. Id. at 567.
119. Id. at 875–86.
120. Id. at 875.
121. Id.
122. Id.
123. Id.
124. O’Leary, 109 So. 3d at 875.
125. Id. at 877.
126. Id.
128. Id. at 1029.
Wise defined “sending” as “the depositing of the communication in the mail or through some other form of delivery” and “receipt of the communication by the person being threatened.” The court held that receipt of a threatening communication by a family member of the person threatened would also fulfill the second prong of Wise’s two-part definition of “sending.”

After analyzing the precedent from Wise, the court in O’Leary concluded that “[w]hen a person composes a statement of thought, and then displays the composition in such a way that someone else can see it, that person has completed the first step in the Wise court’s definition of ‘sending.’” The court found that the defendant “reduced his thoughts to writing” and “placed this written composition onto his personal Facebook page.” The court reasoned that the posting was available for viewing to all of the defendant’s Facebook “friends.” The court looked at Facebook’s mission and found that “there is no logical reason to post comments other than to communicate them to other Facebook users.” By completing the “affirmative act of posting the threats on Facebook,” even though it was on his own personal page, the court held that the defendant sent the post to all of his Facebook friends, including his cousin.

The Statute includes the word “threatens” under “course of conduct.” In 2015, the U.S. Supreme Court heard Elonis v. United

129. Id. at 1030. Section 836.10 is violated when: “(1) a person writes or composes a threat to kill or do bodily injury; (2) the person sends or procures the sending of that communication to another person; and (3) the threat is to the recipient of the communication or a member of his family.” Id.

130. Id.

131. O’Leary, 109 So. 3d at 876.

132. Id. at 877. The court in O’Leary described the “sending” process as follows:

When the threatened individual, or a family member of the threatened individual, views and receives the thoughts made available by the composer, the second step in the Wise definition is completed. At that point, the statement is “sent” for purposes of section 836.10. Further, Internet technologies “generally do not involve communications sent directly to another. Rather, communications are posted for the whole world to see, or, in a closed network for a particular community to see, such as a community of ‘Facebook friends.’”

133. Id. (quoting Jacqueline D. Lipton, Combating Cyber-Victimization, 26 BERKELEY TECH. L.J. 1103, 1127–28 (2011) (footnote omitted)).

134. Id.

136. Id. (explaining that the defendant requested his cousin to be his Facebook friend, a request that the cousin accepted, and that by posting threats directed to his relative on his Facebook page, the court stated that it was reasonable to presume that the defendant wished to communicate that information to all of his Facebook friends).

135. Id.

137. 740 ILL. COMP. STAT. 21/10 (2014).
States and held that the defendant should be criminally charged for posting something “threatening” on his Facebook page. The case centered on the mental state required for a threat to be considered criminal.

In , the defendant, Anthony Elonis, posted threatening messages on social media after his wife left him and took their children with her. One Facebook post read: “‘There’s one way to love ya but a thousand ways to kill ya. I’m not gonna rest until your body is a mess, soaked in blood and dying from all the little cuts,’” The defendant’s wife obtained an order of protection after receiving several other threats from him. The defendant was “convicted of a federal offense and sentenced to more than three years in prison.” He then appealed his conviction.

On June 1, 2015, the Court reversed Elonis’ conviction. The Court held that the prosecution needed to show that Elonis actually intended for the posts to be threats. The Court reasoned that an objective reasonable person standard would not go far enough to separate wrongful conduct from innocent conduct. The Court held that, in this case, an objective standard would risk punishing an innocent actor because the critical element that makes this behavior criminal is the threat, not merely the posting.

G. The Unconstitutional Illinois Cyberstalking Statute

Recently, an Illinois appellate court held that contacting the victim is not enough to violate the Statute. Rather, there needs to be a mens rea requirement incorporated in the Statute that puts the defendant on notice. In June 2016, the Illinois First Circuit Court of Appeals declared portions of the Illinois Cyberstalking Statute to be unconsti-
In _Relerford_, the defendant was convicted of stalking and cyberstalking his former co-worker. The appellate court vacated his convictions, finding that two sections of the Statute were facially unconstitutional because they lacked a mens rea requirement. Because sections (a)(1) and (2) of the general stalking statute and sections (a)(1) and (2) of the Statute contained only a reasonable person standard and no requirement that defendant actually intend to inflict emotional suffering on a person, the court found that they were facially unconstitutional under the Due Process Clause of the Fourteenth Amendment.

The Illinois General Assembly needs to ensure that all forms of stalking are covered under the Statute. By implementing a social media component into the law, the legislature will not only be better able to protect victims of cyberstalking, but will also put social media users on notice of the possible repercussions for posting, searching, or using those sites to stalk others.

### Analysis

To ensure that stalking is handled appropriately, the Illinois General Assembly must ensure that the stalking statutes are relevant and updated. It is important for the General Assembly to research and analyze current stalking statistics across the nation. Moreover, it is important for the General Assembly to understand the role that social media plays in stalking. The Internet has opened up a new domain to stalkers, and it therefore needs to be policed just as heavily as traditional, in-person stalking.

New websites are created every day that make it easier for stalkers to find victims and control them. It is now extremely easy for predators to monitor their victims through de-

---


Subsections (a)(1) and (a)(2) of the cyberstalking statute are virtually identical to subsections (a)(1) and (a)(2) of the general stalking statute. The principal difference is that the cyberstalking statute specifies that the defendant’s course of conduct involved electronic communications. It necessarily follows then, that subsections (a)(1) and (a)(2) of the cyberstalking statute, which also lack a mens rea requirement, are facially unconstitutional under the due process clause of the fourteenth amendment for the same reason that subsections (a)(1) and (a)(2) of the general stalking statute are unconstitutional.

150. Id.

151. Id. at 495–97.


153. Angela Moscaritolo, Facebook Update Makes It Easier to Stalk Your Friends, PCMag (July 9, 2015, 10:28 AM), http://www.pcmag.com/article2/0,2817,2487400,00.asp (“Now it’s even easier to ensure you never miss a Facebook post from your best friend—or frenemy.”).
velopments in a wide range of technology, including global positioning system (GPS) devices.\textsuperscript{154} In order to ensure that the Statute effectively deters cyberstalking, the Illinois General Assembly needs to implement a clear and concise social media component.

The Illinois General Assembly essentially has two choices in terms of amending the Statute; it can impose a strict social media component into the law, which include a mens rea requirement, or explicitly restrict certain avenues of social media from the Statute. By instituting a \textit{strict} social media component into the Statute, constitutional violations are likely to occur.\textsuperscript{155} This Comment proposes a balance between instituting a clear social media component into the Statute and protecting the due process and First Amendment freedom of speech rights of defendants. The General Assembly can add a section to the Statute that specifically addresses social media. This section would put the defendant on notice that intentional contact via social media would constitute a violation of the Statute. The contact must be initiated by the defendant in an effort to convey the message to the victim.\textsuperscript{156} The mens rea requirement is essential to ensuring that the Statute is carried out properly.

This Part analyzes the role that social media plays in relation to stalking, and posits that the Illinois General Assembly needs to update the Statute to include social media and implement a new and separate component to the Statute specifically addressing the requisite mens rea.

\textbf{A. Social Media’s Role in Stalking}

Social media has become increasingly relevant in this technologically advanced world.\textsuperscript{157} One form of social media, Facebook, has become a major avenue for stalkers to stalk their victims.\textsuperscript{158} Facebook is a social media website whose mission is “to give people the power to share and make the world more open and connected.”\textsuperscript{159} However, social media websites, like Facebook, have made it harder to police

\begin{thebibliography}{99}
\bibitem{mensrea} 720 ILL. COMP. STAT. 5/12-7.5 (2014).
\bibitem{facebook} See Grimmelmann, \textit{supra} note 4, at 1168.
\end{thebibliography}
stalking and cyberstalking issues. Because so many people have access to Facebook, it has created endless opportunities for stalking to take place because not all users engage in proper Facebook etiquette. Consider the hypothetical situation in which a user sends friend requests to people they have never met, tries to engage in conversation, and then becomes upset when the stranger does not respond. This scenario begs the question: When does “Facebook stalking” become criminal?

“Facebook stalking” has become an idiom for visiting other users’ Facebook profiles to “browse through their photos, posts, and interactions.” Facebook has made it easier to stalk people by allowing users to have public profiles. Facebook does not have any “privacy” features that can hide the profile picture. Thus, unless the user wants to put a picture of something other than their personal image, or simply a blank image, the entire world has access to the profile picture. Allowing access to this profile picture can give

164. Omer Tene & Jules Polonetsky, A Theory of Creepy: Technology, Privacy and Shifting Social Norms, 16 YALE J.L. & TECH. 59, 100 (2013). The authors, however, make an interesting observation: “Facebook stalking, more generally, is simply using Facebook.” Indeed, who has not rummaged through the photos of an ex-girlfriend or current colleague? Yet the connotation associated with Facebook stalking is clearly negative (e.g., it is not called “Facebook courtesy visiting”); and it is no coincidence that unlike LinkedIn, its business-focused competitor, Facebook keeps information about who visited your profile a closely guarded secret. On LinkedIn, expanded capability to see who has viewed your profile is a premium feature, since social norms for business networking seem to support this type of browsing. The rules of engagement on “stalking” or visiting other profiles have yet to be written. And this further muddles the boundary between ethical and unsavory social media behavior.
166. Id.
167. Id.
stalkers further access to personal images. Moreover, unlike LinkedIn, Facebook hides profile views from its users. So, a stalker could look at his victim’s Facebook page one hundred times per day, and the victim would never know. In its effort to make the world more “open and connected,” Facebook may by its design, though unintended, facilitate stalking.

Because Facebook has become so commonplace, it might be hard for victims of stalking to deactivate their pages. Further, making a victim deactivate her Facebook page seems more like a punishment rather than a safety protection. There is a double standard for victims of cyberstalking. For example, victims of phone harassment are not required to get rid of their phones after being harassed, therefore, why should cyberstalking victims be required to do without their personal social media page? By instituting a strong social media component into the law, society will not have to worry about jeopardizing the victim’s freedoms for safety. A clear and concise social media component will provide further protection for victims from being contacted by their cyberstalkers on social media. The victim may be comforted in the fact that if the cyberstalker violates the Statute, he can be held responsible in a court of law.

There is a common misconception that social media posts marked “private” are in fact private. Facebook allows users to make posts “private” by clicking a button, known as the “privacy check” button, that limits who can view the users’ posts. By clicking “Sign Up,”

---

168. Id.
169. See Facebook vs. LinkedIn—What’s the Difference?, Forbes (May 21, 2012), http://www.forbes.com/sites/joshbersin/2012/05/21/facebook-vs-linkedin-whats-the-difference/#4482217c792f. LinkedIn now allows users to opt out of the viewing preferences under the “Select what others see when you’ve viewed their profile” setting. Kirsten Hodgson, How to View Other People’s LinkedIn Profiles Anonymously, LinkedIn (Oct. 9, 2014), https://www.linkedin.com/pulse/20141009022529-27827108-how-to-view-other-people-s-profiles-anonymously.
170. Tene & Polonetsky, supra note 164, at 100.
171. Id.
174. Ozer, supra note 3.
175. Id.; see also Stokes, supra note 5; see also Michael Osakwe, Facebook’s Privacy Checkup: What Is It and Why Is It Important?, NextAdvisor (Mar. 2, 2016), http://www.nextadvisor.com/blog/2016/03/02/facebook-privacy-checkup/. “The Privacy Checkup helps you review who can see your posts and info from your profile, like your phone number and email address. It also shows you settings for apps you’ve logged into with Facebook.” What’s the Privacy Checkup and How Can I Find It?, Facebook, https://www.facebook.com/help/443357099140264 (last visited Jan. 13, 2017).
However, Facebook warns users that they are essentially entering into a contract accepting Facebook’s terms and admitting having read the Data Use Policy. Facebook’s terms and conditions section informs users that Facebook may use all of the information they receive about the user to serve ads that are more relevant to the user, which includes information provided at registration or added to the user’s account or timeline. Researchers at Carnegie Mellon University determined that it would take the average American seventy-six working days to read all the privacy policies they agreed to each year. It would be unreasonable to expect the average user to read through and understand the entire terms and conditions’ section, especially if it would take them over two months to finish.

Because courts have not said that a reasonable expectation of privacy regarding social media exists, it is even more important that the Illinois General Assembly makes a change to the Statute. Defendants must be aware that any contact, whether direct or indirect, may constitute contact for purposes of the Statute. Victims also need greater protection from any threats that may be communicated to them through social media. By implementing a clear and concise social media component into the Statute, the General Assembly will ensure that defendants are put on notice that “private” social media outlets will still subject them to a violation.

B. Social Media Promotes Stalking

Social media websites, like Facebook, encourage stalking. “Facebook creeping” has become “normal” for users because the site keeps each user’s search history private. Recently, Facebook

177. See id.
178. Mark Sableman, Do You Have Privacy Rights on Social Media?, THOMPSON COBURN (July 12, 2016), http://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2016-07-12/do-you-have-privacy-rights-on-social-media-
179. See Cox, supra note 152.
182. Drake Bennett, Facebook Succeeds Because Deep Down, We’re All Stalkers, BLOOMBERG (May 23, 2014), http://www.bloomberg.com/bw/articles/2014-05-23/the-secret-of-facebooks-success-it-made-stalking-easy (“Facebook leaves users free to peruse others’ content in secret . . . . 80 percent of the clicks on Facebook are related to viewing others’ content, while only 8 percent to 9 percent are related to posting one’s own.”).
has launched an update that allows users to prioritize who they want to see first on their news feeds.183 This feature enables users to handpick who they want to “view” on their newsfeed.184 Not only is this tool helpful for stalkers, but the feature also does not notify those users that someone has added them to their priority list.185 Therefore, by allowing users to anonymously creep through fellow Facebook users’ profiles, Facebook is passively promoting cyberstalking.186

Facebook stalking has also become increasingly relevant as a coping method following relationship break-ups.187 After a break-up, an individual can constantly view their ex-partner’s Facebook page hundreds of times a day, essentially monitoring their every move.188 This anonymous access to an ex-partner’s Facebook profile may lead to obsessive tendencies that eventually turns into stalking.

Facebook stalking can have a huge impact on relationship intrusion, it is important for the Illinois legislature to incorporate a social media component into the Statute.189 Research has shown that Facebook stalking is becoming more prevalent and consistently leads to dangerous outcomes for the victims.190 If the General Assembly were to address the ramifications of cyberstalking, it might create a deterrence effect on Facebook stalking.

184. Id.
185. Id.
186. See Topping, supra note 180.
188. Marlynn Wei, How to Keep Social Media from Complicating Your Relationship, Psychol. Today (Jan. 25, 2015), https://www.psychologytoday.com/blog/urban-survival/201501/how-keep-social-media-complicating-your-relationship. Researchers have identified aspects of social media sites that “make them more prone to relationship surveillance”:
1. Information is easily accessible. Even if a profile isn’t public, it’s likely that it’s shared with a person’s partner or available via mutual friends.
2. People post a wide variety of media, ranging from photos and videos to links. Photos can communicate a lot of information about location, behaviors, and social interactions.
3. Social media profiles archive a significant amount of past information. How often do people delete old photos from their Instagram feed from two or three years ago? Probably not that often. Editing posts is tedious, and people would lose their posting history, making it even less likely that they will want to remove old data.
4. Data can be gathered secretly. Most social networking sites do not give you reports on who is looking at your information or how often.
    189. See Ghose, supra note 187.
Implementing a social media component into the Statute will ensure that victims of stalking have protection from any and all types of unwanted contact, including through electronic platforms such as social media. Because victims are often denied justice in cyberstalking cases, it is not surprising that they have little confidence in the legal system. In the face of waning confidence, the Illinois General Assembly must ensure that these victims are protected in all foreseeable situations.

If the Statute is not amended to have a clear and all-encompassing social media component, the public will not know what constitutes a violation under the Statute. Technology is ever changing and so are social media websites. It is hard enough for users to keep up with the constant application updates, let alone the underlying meaning of the terms and conditions sections. Therefore, unless the Statute is clear and all encompassing, defendants will likely be in the dark in relation to social media violations.

C. Indirect Stalking

What most stalkers fail to realize is that stalking does not have to be direct contact. Stalking incudes posting on social media, posting on personal accounts, and posting information concerning the victim, which the victim may not have access to or cannot view. Although no case law on stalking order violations exists in Illinois, the broad consensus among different jurisdictions is that almost any type of contact, direct or indirect, will constitute a violation of the relevant stalk-
ing legislation.\footnote{197 Terry O’Malley, Social Media Sites Can Cause Protection/Restraining Order Violation in Larimer County, O’MALLEY LAW OFFICE P.C. (Sept. 3, 2013), http://www.criminaldefensefortcollins.com/social-media-restraining-order-violation/} As in Craig, even though the defendant did not communicate directly with the victim, he was still held in violation of the order.\footnote{198 New Hampshire v. Craig, 112 A.3d 559, 566 (N.H. 2015).}

In Craig, the New Hampshire Supreme Court interpreted “contact,” in the stalking context, to include posting messages on social media.\footnote{199 \textit{Id.}} A broad interpretation of the Statute would entitle victims protection from stalking throughout all forms of communication.\footnote{200 Id.} However, in order for the Statute to be effective, it must be clear. As currently written, the Illinois Cyberstalking Statute is ambiguous as to what types of social communication are considered “contact.”\footnote{201 720 ILL. COMP. STAT. 5/12-7.5 (2014).} The point behind having a broad statute is to ensure that victims are protected. A broad statute would also ensure that there are not any loopholes for defendants to get access to the victim.\footnote{202 John F. Decker & Peter G. Baroni, “No” Still Means “Yes”: The Failure of the “Non-Consent” Reform Movement in American Rape and Sexual Assault Law, 101 J. CRIM. L. \\& CRIMINOLOGY 1081, 1128 (2011).} However, the Illinois General Assembly cannot create broad statutes that impinge on the constitutional rights of American citizens. Defendants must be aware of what type of actions are considered “contact.”

The New Hampshire statute in Craig specifically lists “any form of electronic communication” in its list of “actions to communicate.”\footnote{203 N.H. REV. STAT. § 173-B:1 (2016).} “Contact” means any action to communicate with another either directly or indirectly, including, but not limited to, using any form of electronic communication, leaving items, or causing another to communicate in such fashion.”\footnote{204 \textit{Craig}, 112 A.3d at 566.} The New Hampshire Supreme Court found that this mention of electronic communication “reflected the legislature’s awareness of technological advances in communication.”\footnote{205 \textit{Id.} at 567.} The court explained that when a person “composes a statement of thought, and then displays the composition in such a way that someone else can see it” that person has completed the first step in sending the message through social media.\footnote{206 \textit{Id.} at 568.} Furthermore, by posting the message on a social media outlet, the court ruled that there was “‘no logical reason’ for the defendant to post statements directed to the victim on Facebook other than to communicate them.”\footnote{207 \textit{Craig}, 112 A.3d at 566.} Therefore, the court ultimately held that personal posts on a social media outlet constitute “contact” for the
purpose of a stalking statute, even when the stalker does not intend for the victim to view it or allow her to view it on his page.\footnote{207} In \textit{Craig}, the statute was specific enough for courts to interpret it in this manner. Illinois should adopt this interpretation by implementing a specific social media component into the law.\footnote{208}

Although Illinois courts have not decided whether a personal post on a social media site can constitute “contact” or “sending” for the purpose of the Statute, it is likely that if a case were to arise, the court would likely hold that those posts do constitute “contact.”\footnote{209} If a defendant were to post a threatening message on his Facebook page concerning someone else (not a Facebook friend), Illinois courts may be inclined to follow the reasoning in \textit{O’Leary} and determine that the message constitutes indirect contact. Because technology is constantly changing, it is the duty of the legislature to keep up and amend or update existing laws.\footnote{210} If the Illinois General were to adopt this interpretation of contact in terms of violating the Statute, it would be their obligation to ensure that defendants are put on notice. This means that the General Assembly would need to update the current Statute with a specific social media component that addresses not only direct versus indirect contact, but also contact that might occur on a private social media page.

In \textit{O’Leary}, even when a defendant was not friends with the victim, the court still held his communication to be contact.\footnote{211} The distinction between Facebook friend verses Facebook user is important, especially when dealing with violations of an order of protection.\footnote{212} If the defendant’s Facebook page is private, and he is not Facebook friends with the victim, the victim cannot through her own Facebook page, see anything the defendant posts. It is possible that the defendant might not even intend to communicate his private posts to the victim. By holding that all private posts on Facebook constitute communicating with every user on the Facebook network, the court seems to be taking an insurmountable leap to impute liability on the defendant.\footnote{213}

\begin{flushleft}
\footnote{207}Id. at 566. \\
\footnote{208}Id. \\
\footnote{210}Vivek Wadhwa, \textit{Laws and Ethics Can’t Keep Pace with Technology}, MIT TECH. REV. (Apr. 15, 2014), http://www.technologyreview.com/view/526401/laws-and-ethics-cant-keep-pace-with-technology/ (“The gaps are getting wider as technology advances ever more rapidly. And it’s not just in employment and lending—the same is happening in every domain that technology touches.”). \\
\footnote{211}\textit{O’Leary}, 109 So. 3d at 877. \\
\footnote{212}Id. \\
\footnote{213}Id.}
\end{flushleft}
Regardless of whether Facebook is really “private,” the defendant in O’Leary did not intend for the victim to view his comments. He did not intend to communicate with all Facebook users. The court was essentially trying to equate his behavior to that of someone standing on a street corner holding up a sign containing a nasty comment concerning a victim. Because social media sites like Facebook have become so commonplace, it is important for the legislature to take that into account and amend the Statute to ensure that defendants are aware of what would constitute communication via social media.

D. Is the Statute Valid?

The Statute, as written, is vague and it therefore violates a defendant’s right to due process. A statute is void for vagueness if it “fails to give a person of ordinary intelligence a reasonable opportunity to know what is prohibited.” The void-for-vagueness doctrine is used when the statutory standards are so undefined that courts “cannot apply a criminal statute without engaging in common law rulemaking.”

As it currently stands, a course of conduct is defined as any acts in which a defendant “directly, indirectly or through third parties . . . follows, monitors, observes, surveils, threatens or communicates to or about” the petitioner. Although the Statute mentions “electronic” communication, it can be argued that posting on a “private” social media website, in which the petitioner is not able to view, does not constitute communicating. The Statute appears to be broad and all

214. Id. at 875.
215. Id.
216. Id.
217. O’Leary, 109 So. 3d at 495–96.
218. Valle del Sol Inc. v. Whiting, 732 F.3d 1006, 1019–20 (2013) (quoting Hunt v. City of Los Angeles, 638 F.3d 703, 712 (9th Cir. 2011)). A statute is only facially void for vagueness if it is vague “not in the sense that it requires a person to conform his conduct to an imprecise but comprehensible normative standard, but rather in the sense that no standard of conduct is specified at all.” Id. at 1020.
219. Brian Slocum, RICO and the Legislative Supremacy Approach to Federal Criminal Lawmaking, 31 Loy. U. Chi. L.J. 639, 640 (2000). The Supreme Court has indicated approval of related doctrines. In United States v. Lanier, 520 U.S. 259 (1997), the Court described the “three related manifestations of the fair warning requirement” of due process. Lanier, 520 U.S. at 266 (explaining that to prevail on a vagueness challenge, the challenger must demonstrate that: (1) a person of ordinary intelligence would not have a reasonable opportunity to understand what conduct the statute prohibits; or (2) the statute authorizes or encourages arbitrary enforcement).
220. Lanier, 520 U.S. at 266.
221. Id.
encompassing, including communication “directly or indirectly” and “through third parties.” However, that language is vague.

The Statute is vague because it does not include the words “social media.” Because the Fourteenth Amendment provides defendants with due process, they must be put on notice with unambiguous language that any communication via a social media outlet can and will subject them to jurisdiction under the Statute. This would clarify the “electronic communication” element by specifically addressing the social media component. The Statute also does not have a mens rea requirement. In Relerford, the court specifically noted that, as currently written, the Statute contains a reasonable person standard and no requirement that defendant actually intend to inflict emotional suffering on a person. The reasonable person standard in a criminal statute is unconstitutional. There is no statute defining the term “reasonable person” in stalking or harassment criminal offenses. Therefore, the Statute should focus on the intent of the perpetrator rather than the impact on the victim. It should also establish a clear mens rea element and avoid any infringement on a defendant’s due process rights.

The question that remains is whether or not a reasonable person would understand that the Statute prohibits Facebook users from posting information concerning victims on their own private page. Social media sites that provide “privacy tools” give users a false sense of security. Many social network users assume some degree of privacy within their circle of friends. However, whether Facebook users are aware that this is a false sense of security is the question at issue.

E. Facebook Lacks Privacy

When people in relationships break up and start posting nasty things about their ex-partner on their own Facebook page, they cannot expect those posts to be private. Even though Facebook has

222. Id.
223. Id.
226. Id. at 495–96.
227. Id. at 495.
228. Id.
229. See Ozer, supra note 3.
231. Id.
232. Id.
put “privacy” features in place, those features give the average user a false sense of security.\footnote{233. Ozer, supra note 3.} In order to prevent potential stalking defendants from violating the Statute by posting information related to the victim, the Illinois General Assembly needs to ensure that it clearly addresses the ramifications if the defendant posts anything relating to the victim on any social media outlet, regardless of whether their account is private.

Many people who post things on their “private” Facebook page expect that whatever they post will remain confidential.\footnote{234. Danielle Matterson, \textit{Is My Facebook Page Really Private?}, \textsc{Stoneham Patch} (Mar. 5, 2014, 3:49 PM), http://patch.com/massachusetts/stoneham/is-my-facebook-page-really-private.} Unfortunately, that is not the case.\footnote{235. Id.} Although Facebook’s privacy policy claims to limit the availability of its user’s information to third parties, it also states that Facebook may “access, preserve, and share” that information in response to a legal request, to address fraud, or to “protect” itself.\footnote{236. \textit{Policy Statement}, \textsc{Facebook}, https://www.facebook.com/policy.php (last visited Mar. 1, 2016).} Facebook’s privacy statement is extremely broad and all encompassing.\footnote{237. Id.} However, under the Third Party Doctrine, anything posted on Facebook, or social media in general, is subject to seizure by the government.\footnote{238. Id.} The Third Party Doctrine is the Fourth Amendment rule that governs the collection of evidence from third parties in criminal investigations.\footnote{239. Orin S. Kerr, \textit{The Case for the Third-Party Doctrine}, 107 \textsc{Mich. L. Rev.} 561, 563 (2009).} The rule is simple: “By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed.”\footnote{240. Id.} Pursuant to \textit{Smith v. Maryland}, the Fourth Amendment does not apply to information held by a third parties like Facebook.\footnote{241. Id. at 743–45; see also \textit{Smith v. Maryland}, 442 U.S. 735, 744 (1979).} In \textit{Smith}, the U.S. Supreme Court extended the Third Party Doctrine to include information voluntarily disclosed to automated machines.\footnote{242. \textit{See Smith}, 442 U.S. at 744; \textit{see also} Monu Bedi, \textit{Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply}, 54 \textsc{B.C.L. Rev} 1, 3 (2013).} The court held that government only
needs a subpoena to obtain your personal information held by third parties, like Facebook. The reasoning in Smith can be directly applied to social media. The Court essentially states that social media users do not have a reasonable expectation of privacy when posting things on third party websites.

The Facebook generation, as it has come to be known, is commonly used to “identify those who are growing up in a world where the use of online social networking is common.” Many Facebook users tend to post hundreds of statuses detailing their daily routine, pictures of what their day consists of, and the current status of their romantic relationships. Social media has fundamentally changed the way we communicate. Years ago, technology did not give people the opportunity to interact with others the way it does today. People had to go outside their comfort zones to meet new people. Social networking sites, on the other hand, allow people to simply open the app on their smart phone and stare at what their family members or friends are doing for hours. Social media has virtually done away with face-to-face interaction. It allows people to “socialize” behind a computer screen.

Because social media has become ubiquitous, social media users have a false sense of security when it comes to privacy. What someone from the Pre-Facebook Generation may view as “contact,” current active Facebook users may not. Moreover, active Facebook users may reasonably expect that information they post on their “pri-

\textit{Id.} at 3.


244. \textit{Id.} at 744.

245. See Bedi, supra note 242.


250. \textit{Id.}

251. See Bates, supra note 248.

252. \textit{Id.}

253. See Ozer, supra note 3.

254. Anick Jesdanun, \textit{Facebook Resisters, Why Some Just Refuse to Join}, \textsc{Assoc. Press} (May 17, 2012), \url{http://www.thestar.com/business/2012/05/17/facebook_resisters_why_some_just_refuse_to_join_the_social_network.html}.
vate” accounts remains private.\textsuperscript{255} Given the fact that Facebook provides privacy controls, it seems reasonable for users to have some sort of privacy expectation.\textsuperscript{256} In order to prevent the Statute from being declared vague, the Illinois General Assembly should add a section that specifically deals with social media.

Social media has become a powerful tool for dispensing threats.\textsuperscript{257} Many social media users utilize Facebook and other online forums as their own personal journal.\textsuperscript{258} Some users confide in their Facebook friends and sometimes post emotional comments that may or may not be a reflection of their true intentions.\textsuperscript{259}

In \textit{Elonis}, the United States Supreme Court held that the prosecution needed to show that the defendant intended the posts to be threats.\textsuperscript{260} This holding was controversial, especially for victims of domestic violence.\textsuperscript{261} Many people believe that when it comes to domestic violence or stalking, law enforcement should err on the side of caution.\textsuperscript{262} However, this is the United States of America and citizens have constitutional rights, particularly freedom of speech.\textsuperscript{263} The Court explained that an objective reasonable person standard would not go far enough to separate innocent, accidental conduct from purposeful, wrongful acts.\textsuperscript{264} The holding in \textit{Elonis} is especially important when deciding whether or not to amend the Statute.\textsuperscript{265} Currently, the Statute does not incorporate a mens rea element under the course of conduct section.\textsuperscript{266} As the Statute is currently written, consider for example that a defendant can post threatening rap lyrics on his Facebook page regarding the victim and be in violation of his order, regardless of whether or not he intended to pursue the

\begin{thebibliography}{99}
\bibitem{255} See Ozer, supra note 3.
\bibitem{256} Id.
\bibitem{261} Soraya Chemaly & Mary Anne Franks, \textit{Supreme Court May Have Made Online Abuse Easier}, TIME (June 3, 2015), http://time.com/3903908/supreme-court-elonis-free-speech/.
\bibitem{262} Id.
\bibitem{263} U.S. \textit{Const.} amend. I.
\bibitem{264} \textit{Elonis}, 135 S. Ct. at 2003.
\bibitem{265} Id.
\end{thebibliography}
threats. If the Illinois General Assembly decides to incorporate a social media component into the Statute, it should also include the mens rea requirement. Without that requirement, defendant’s constitutional rights will be at risk.

The vagueness of the Statute not only detrimentally affects victims of stalking, but it also puts the constitutional rights of defendants in jeopardy. The Statute should be amended to ensure that those threats are included within the “electronic communication” section because social media has become a powerful tool for dispensing threats. Respondents to stalking orders may use social media as a personal journal private from the rest of the world.

A “reasonable person” might believe that private social media profiles are, in fact, private. However, if the Statute was clear and left no room for questioning, defendants would be on notice that anything they post on social media can be used against them. A clear statute would incorporate social media and privacy features into the language. For example, the Statute would list social media as a form of electronic communication. The Statute would further state that this section applies to any and all posts to social media websites, including private posts.

IV. Impact

Stalking is a serious and relevant problem for countless victims nationwide. Victims of stalking need to know that they will be protected from all forms of stalking, whether direct, indirect, in person or online. Equally important is the need to put defendants on notice to protect their due process rights. Resolving the vague components of this Statute will absolutely ensure that both victims and defendants are protected. Although an amendment may not solve the problem of cyberstalking, it will give victims an outlet to voice their concerns and pursue justice.

268. See Mens Rea–A Defendant’s Mental State, supra note 266.
272. Id.
273. Id.
274. Id.
275. Id.
276. Id.
277. See Levin, supra note 23.
Social media facilitates stalking. Sites like Facebook, Twitter, and Myspace allow users to anonymously search through personal pages and essentially monitor what others are doing. Because social media has become part of the “norm,” the Illinois General Assembly needs to ensure that stalking legislation is keeping up with advancements in technology. The Illinois General Assembly can help protect victims of cyberstalking by implementing a specific social media component into the Statute.

Social media can help facilitate stalking because it is a popular mode of communicating directly with others in today’s society. Each and every day, millions of people sign-in to sites like Facebook and Twitter to communicate with others. This instant form of communication makes it easier for stalkers to stalk their victims. It is important that those victims are protected. In order to ensure that they are protected, the Illinois General Assembly needs to update the Statute to include communication via social media. This will guarantee that all social media users are aware that anything they post on their “personal” webpage is not private and can be used against them in a court of law.

B. Impact on Defendants

Clear and all-encompassing cyberstalking legislation will ensure that a defendant’s procedural due process rights are guaranteed. Defendants are entitled to a constitutionally adequate procedure when the government aims to rescind one of their liberties. As it stands now, an Illinois appellate court has declared a portion of the Statute unconstitutional for lack of a mens rea component. Therefore, it is vital that the legislature make a swift and concise change to the law. By instituting a requirement that the defendant actually intend to in-
flict emotional suffering on a person, the General Assembly will protect the due process rights of the defendants.

C. Impact on Freedom of Speech

The General Assembly has two options to reconstruct the Statute. It can impose specific social media components into the law, which include a mens rea requirement, or explicitly restrict certain avenues of social media from the Statute. Instituting a strict social media component to the law may violate the defendant’s First Amendment right to freedom of speech. Specifically, when a defendant is posting information on his private account, his speech may be protected under the First Amendment.

In Elonis, the Supreme Court held that there must be a subjective intent behind the alleged threatening communication. This subjective intent requirement separates wrongful conduct from innocent conduct. By instituting a strict social media component, the General Assembly might hinder the defendant’s right to free speech and subsequently misconstrue his intentions. If the defendant posts a message about the victim on his private Facebook page, he is not contacting the victim. His actions could not constitute direct or indirect contact because he is not actively trying to send the message to the victim. The victim would have to go out of her way to view the message, and the only way this situation could constitute a violation of the Statute would be if the defendant solicited someone to relay the message to the victim. That would constitute indirect contact and he would be in violation of the Statute. In that situation, the defendant is going out of his way to reach the victim which is completely different than posting a message on his private page in which he is not friends with the victim and has no intentions of having the victim see his message.

D. Plans for the Future

If the Illinois General Assembly institutes a strict social media aspect to the current Statute, constitutional violations are bound to oc-
The legislature can add a section to the Statute that specifically addresses social media. This section would protect the due process rights of the defendant by putting him on notice that intentional contact via social media would constitute a violation. The mens rea requirement is vital to ensuring the statute is carried out properly and void of any constitutional violations. The contact must be initiated by the defendant with the intent of conveying the message to the victim.

E. Impact of Stalking

The impact of stalking may vary depending on the different circumstances that apply to the situation. Stalking can have a tremendous impact on the victim’s mental and physical health. Victims often report feeling fearful of being alone or harmed again in the future. Many victims often report feelings of depression and difficulty sleeping, and some victims never feel a sense of normalcy after being stalked.

Recently, Erin Andrews, a famous sports broadcaster, came forward discussing how her experience as a victim of stalking has severely impacted her life. In 2008, Andrews was staying at the Marriot Nashville while covering a football game. Her stalker, Michael Berret, checked into the room next to her and tampered with the peephole attached to her hotel door. He then shot a video of her changing her clothes and posted it on the internet. During the trial, Andrews explained how the release of the video has impacted

---

295. Id.
296. 720 ILL. COMP. STAT. 5/12-7.5.
297. Impact of Stalking on Victims, STALKING RISK PROFILE, https://www.stalkingriskprofile.com/victim-support/impact-of-stalking-on-victim (last visited Mar. 3, 2016). The impact of stalking may vary according to the victim’s characteristics, past experience, current circumstances, and what they know, or don’t know, about the stalker. Id.
298. Id.
299. Id.
300. Id.
302. Id.
303. Id.
304. Id.
her life. 305 Her testimony was powerful and is a good example of the pain and despair that victims of stalking may face. 306

The General Assembly needs to ensure that victims like Andrews are protected from harassment via social media. By implementing a social media section into the Statute, victims will have the protection that they need. 307 Many social media users fail to realize that posting on personal accounts and posting “private” information concerning the victim may constitute contact, so a section directly addressing social media would address those concerns. 308 Although no case law on stalking order violations exists in Illinois, the broad consensus among different jurisdictions is that almost any type of contact, direct or indirect, will constitute a violation. 309 Like in New Hampshire v. Craig, even though the defendant did not communicate directly with the victim, he was still held in violation of the order. 310

The failure to implement these changes would have the greatest impact on the victims. 311 As the law currently stands, social media is not addressed at all. 312 Although “electronic communication” is mentioned, it is not clear what constitutes electronic, let alone “communication.” 313 Therefore, victims that feel violated by a communication done via social media may not have a viable claim in court. 314 This would leave them susceptible to online harassment, cyberstalking, and overall insecurity. 315

If the Illinois General Assembly implements a social media component to the Statute, it will clear up potential litigation issues and give everyone a stronger sense of security. Defendants will be put on notice of the possible violations that can occur when using social media websites, be those private or public. 316 In addition, victims will also be protected because they will be able to come to court and bring a viola-

305. Id. ("The day that I got the phone call that this was on the Internet, I didn’t want to get undressed. I didn’t change my clothes for two or three days. I was so screwed up. I was disgusted with myself; I was disgusted with my body, with being naked, and that everybody saw that it was me.").
306. Id.
307. Finn, supra note 301.
308. See Quarmby, supra note 192.
310. See Craig, 112 A.3d at 566.
311. See supra note 48 and accompanying text.
312. See 720 Ill. Comp. Stat. 5/12-7.5.
313. Id.
314. Id.
316. Id.
tion if they feel the Statute was violated via social media. Overall, in order to get with the times and ensure the safety and well-being of its citizens, the Illinois General Assembly should address and implement a clear and concise social media component to the Statute.

V. Conclusion

Stalking legislation in Illinois needs to be updated to ensure that victims are protected from cyberstalking done via social media and that defendants constitutional rights are not violated. If the General Assembly conducts thorough research on the topic of cyberstalking, it will find that it has become a huge problem throughout the years.

The problem with the current law is that social media is not addressed at all. Although the Statute does mention “electronic communication,” many social media users would not consider personal posts on social media to be considered “communication.”

The Illinois General Assembly should implement a strict social media component as soon as possible and take a proactive approach to avoid future legislation. In doing so, defendants will be put on notice. Furthermore, victims of stalking will have a form of redress for cyberstalking abuse. By taking a proactive approach to closing loopholes in the Statute, Illinois will be on board with many other states. Amending the Statute will be a fair and effective method of reform that is vital to prevent confusion and promote protection.

Gina Leahy*

---

317. Id.
318. Id.
321. Id.

* J.D. Candidate 2017, DePaul University College of Law. I want to thank Emily Koza, Esq. for her thorough and thoughtful edits of this Comment. In addition, I would like to thank the DePaul Law Review Volume 66 Editorial Board for their invaluable help and guidance. Lastly, I want to thank my family for their endless support and encouragement.