Northern Illinois University Law Review

Volume 36 | Issue 3 Article 4

7-1-2016

Prosecuting Threats in the Age of Social Media

Enrique A. Monagas

Carlos E. Monagas

Prosecuting Threats in the Age of Social Media

ENRIQUE A. MONAGAS[1]
CARLOS E. MONAGAS[2]

Social media has opened new avenues for perpetrators to threaten and intimidate. No longer does someone need to physically stalk their prey to deliver a message; they can now threaten anyone, anywhere with just one click of their cell phone. And because the threatening communications are often prepared in private and can be delivered anonymously, they are not regulated by social norms that would harshly condemn such behavior. Thus, it should come as little surprise that threats are increasing every year and online threats are fueling that growth. This Article considers the challenges facing prosecutors in charging and prosecuting online threats after the Supreme Court's decision in Elonis v. United States, 135 S. Ct. 2001 (2015). Social media has radically changed the way we communicate, removing both in-person human interaction and the meaning and intent such interaction conveys. In this Article, we argue that applying the recklessness standard to today's online communications has the unjustified danger of punishing legitimate speech without increasing public safety.

1. Enrique A. Monagas, Associate Attorney, Gibson, Dunn & Crutcher LLP. Mr. Monagas concentrates his practice on appellate, constitutional law, crisis management, and complex litigation matters.

2. Carlos E. Monagas, Supervising Deputy District Attorney, Office of the District Attorney for Riverside County. The authors would like to thank Stephen Herndon, Esq. and Sean O'Neill, Esq. for their invaluable assistance.

I. INTRODUCTION

Can you tell the difference between a joke and a threat? When do creative rap lyrics become a vehicle for intimidation? When does a Facebook post transform into a terrorist act? Every day millions of communications are sent via social media. Celebrated new forms of electronic communication have brought people together in new and profound ways. But there lurks a troubling side to this medium: social media has become a preferred conduit for threats and criminal intimidation. Regrettably, people are willing to say things online that they would never say in person, face-to-face.

But simply reading an online comment or message board often does not provide sufficient context. "Is what I just read a threat or is the writer being sarcastic?" Jokes and offensive comments are commonplace and often spontaneous in this medium. Additionally, communications intended for just a few may inadvertently reach millions. A person's intent can well be lost in translation. In all events, joke or not, social media communications that are interpreted by recipients as threats do cause real harm. The fear that threats engender can have profound detrimental consequences for victims.

Regardless of the personal wishes of the declarant, these communications may in fact create actual victims.

Consider a pending case from Texas.[3] Two teenagers playing an online video game start arguing on an online chat room.[4] Their private argument spills onto Facebook, where by the nature of the social media platform, their back-and-forth exchange is distributed to hundreds of people who are not part of their conversation and lack any and all context.[5] At one point, one of the teenagers calls the other "crazy." In response, the other teenager replies sarcastically, "I'm fucked in the head alright. I think I'ma (sic) SHOOT UP A KINDERGARTEN AND WATCH THE BLOOD OF THE INNOCENT RAIN DOWN AND EAT THE BEATING HEART OF ONE OF THEM."[6] Unbeknownst to either teenager, a third person in Canada (a complete stranger) views the postings and believes that a deranged shooter is planning to attack an elementary school.[7] In light of the horrific and senseless murders at Sandy Hook Elementary School that had occurred less than two months prior,[8] she finds the threat credible and terrifying. She takes a cell-phone screenshot of the comments, informs the police, and the teenager is promptly arrested and charged with making terroristic threats—a felony that could bring a sentence of up to eight years.[9] Should a careless teenager be allowed to freely say whatever he wants online? What should concerned social media users do when they perceive a credible threat of violence? How should law enforcement agencies respond?

Online threats have real-world consequences. Policing threats, however, must be balanced with the First Amendment's right to free speech. Although the Supreme Court has recognized a "true threats" exception to the freedom of speech—permitting a state to ban "those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals"[10]—whether a declarant must *subjectively* desire to threaten someone to be found outside First Amendment protection is a question the Court has

---

3. Doug Gross, *Teen in jail for months over 'sarcastic' Facebook threat*, CNN (July 3, 2013, 7:18 AM), http://www.cnn.com/2013/07/02/tech/social-media/facebook-threat-carter/index.html.

4. *Id.*

5. *Id.*

6. Craig Malisow, *The Facebook Comment That Ruined a Life*, DALL. OBSERVER (Feb. 13, 2014), http://www.dallasobserver.com/news/the-facebook-comment-that-ruined-a-life-6431863.

7. Gross, *supra* note 3.

8. Devlin Barrett & Tamer El-Ghobashy, *Dozens Killed in Conn. School Shooting*, THE WALL STREET JOURNAL (Dec. 17, 2012), http://www.wsj.com/articles/SB10001424127887323297104578179271453737596.

9. Gross, *supra* note 3; Malisow, *supra* note 6.

10. Virginia v. Black, 538 U.S. 343, 359 (2003).

yet to resolve.[11] Yet, the answer to this question is critically important to state legislatures and local law enforcement agencies who must respond to the seeming explosion of online threats.

In 2015, it appeared that the Court was prepared to answer this intent question. In *Elonis v. United States*, the Court considered "[w]hether, consistent with the First Amendment . . . conviction of threatening another person requires proof of the defendant's subjective intent to threaten."[12] At issue was a defendant's federal conviction for online harassment under 18 U.S.C. § 875(c), which makes it a federal crime to "'transmit[] in interstate or foreign commerce any communication containing . . . any threat to injure the person of another.'"[13] The defendant had been convicted under a "reasonable person" standard, which allowed for conviction if the evidence demonstrated that a reasonable person would regard the statement as threatening.[14] Whether the defendant *actually* sought to threaten his victim was not relevant under this objective, general intent standard.

Instead of considering the First Amendment principles at play, however, the Court sidestepped the constitutional issues and decided the case on a statutory basis. Specifically, the Court held that in "interpreting federal criminal statutes that are silent on the required mental state, we read into the statute 'only that *mens rea* which is necessary to separate' wrongful conduct from 'otherwise innocent conduct.'"[15] Here, mere negligence would not suffice.[16] As such, a defendant needed to act with some higher level of culpable awareness to be convicted. Because the court below erred when it used a negligence standard, the conviction was reversed.[17] Of consequence, however, the Supreme Court did not determine which level of culpability was necessary for conviction under the federal statute. Whether purposefulness or knowledge was required, or whether recklessness alone would suffice, was left for another day. Nor did the Court have reason to answer a threshold question Justice Ginsberg posed at oral argument:

> How does one prove what's in somebody else's mind? This case, the standard was would a reasonable person think that the words would put someone in fear, and reasonable people can make that judgment. But how would the government prove

11. *See* Elonis v. United States, 135 S. Ct. 2001 (2015).
12. Petition for Writ of Certiorari at (I), Elonis v. United States, 135 S.Ct. 2001 (2015) (No. 13-983).
13. Elonis v. United States, 135 S.Ct. 2001, 2008 (2015).
14. *Id.*
15. *Id.* at 2010.
16. *Id.* at 2012-13.
17. *Id.* at 2013.

> whether this threat in the mind of the threatener was genuine?[18]

This paper considers the questions left open in *Elonis*. Part II of this paper provides an overview of social media and considers why it has become a fertile ground for threats and intimidation. Part III briefly traces the history and reasoning underpinning the various levels of criminal culpability. Part IV provides an analysis and roadmap to proving intent under the culpability levels set forth in *Elonis*. Part V considers how a prosecutor should balance public safety and free speech when charging social media threats. Finally, Part VI considers recklessness culpability in the age of social media. Social media has radically changed the way we communicate, removing both in-person human interaction and the meaning and intent such interaction conveys. We argue that applying the recklessness standard to today's online communications has the unjustified danger of punishing legitimate speech without increasing our public safety.

II. SOCIAL MEDIA OVERVIEW

There is a new world order.[19] And it seems to have passed people of a certain age right by.[20] Online communication—or social media—has quickly become the preferred method to connect and communicate for many Americans, and especially for those under thirty.[21] Indeed, living in the "real world" today requires constant access to computers or mobile devices just to keep up: your colleagues get their news from Facebook, relatives constantly post new photos on Instagram, children speak to their friends through videos on Snapchat, friends gossip on Twitter, and so on.

---

18. Transcript of Oral Argument at 4-5, Elonis v. United States, 135 S. Ct. 2001 (2015) (No. 13-983).

19. Nick Jones, *Social Media and the New World Order*, THE HUFFINGTON POST (June 25, 2013), http://www.huffingtonpost.co.uk/nick-jones/social-media-and-the-new-world-order_b_3477545.html ("People, and particularly younger people, are increasingly choosing to miss out [sic] the political class and the mainstream media altogether, connecting with each other directly to form political movements and make their voices heard.").

20. *See* Frank Newport, *The New Era of Communication Among Americans*, GALLUP (Nov. 10, 2014), http://www.gallup.com/poll/179288/new-era-communication-americans.aspx ("The use of social media to communicate is in the top four among those aged 18 to 29, but its use drops off significantly among those 30 or older.").

21. *Id.*

A. AN INTRODUCTION TO TODAY'S MOST USED SOCIAL MEDIA PLATFORMS

Facebook describes itself as a tool that gives "people the power to share and make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."[22] Presently, it is the dominating social media platform.[23] Users are identifiable on Facebook and are able to disseminate their messages to the world broadly—or discretely to friends and strangers alike through private messages.

Instagram describes itself as a "way to share your life with friends through a series of pictures."[24] Through the application software,[25] users can take photos on their mobile devices, "then choose a filter to transform the image into a memory to keep around forever."[26] For today's teenagers, Instagram is the most used social media outlet.[27] Alarmingly, many articles have been written on the coded language of Instagram and how it can be a tool to achieve or destroy social statuses and self-esteem among teens.[28]

Twitter enables its users to send and read short 140-character messages called "tweets." Through these short declarations transmitted electronically to the entire world, Twitter aspires to "give everyone the power to create and share ideas and information instantly, without barriers."[29] In practice, Twitter has been best used as a way to deliver news or sell products.[30]

---

22. FACEBOOK MISSION STATEMENT, https://www.facebook.com/facebook/info/?tab=page_info (last visited Jan. 14, 2016).

23. AMANDA LENHART, TEENS, SOCIAL MEDIA & TECHNOLOGY OVERVIEW 2015 (Pew Research Center 2015).

24. INSTAGRAM FAQ, https://www.instagram.com/about/faq/ (last visited Jan. 14, 2016).

25. Hereinafter, "app."

26. INSTAGRAM FAQ, *supra* note 20.

27. Andrew Watts, *A Teenager's View on Social Media*, MEDIUM (Jan. 2, 2015), https://medium.com/backchannel/a-teenagers-view-on-social-media-1df945c09ac6#.5gd733lo1.

28. *See, e.g.*, Rachel Simmons, *The Secret Language of Girls on Instagram*, TIME (Nov. 10, 2014), http://time.com/3559340/instagram-tween-girls/; Jessica Winter, *Selfie-Loathing*, SLATE (July 23, 2013), http://www.slate.com/articles/technology/technology/2013/07/instagram_and_self_esteem_why_the_photo_sharing_network_is_even_more_depressing.html.

29. TWITTER MISSION STATEMENT, https://about.twitter.com/company (last visited Jan. 14, 2016).

30. *See* Yoree Koh, *Twitter Unveils Curated News Feature 'Moments'*, THE WALL STREET JOURNAL (Oct. 6, 2015), http://www.wsj.com/articles/twitter-with-dorsey-as-ceo-unveils-curated-news-feature-moments-1444136401; *see also* Deepa Seetharaman, *What Celebrities Can Teach Companies About Social Media*, THE WALL STREET JOURNAL (Oct.

Snapchat allows users to share images, videos, and text that are then automatically deleted within a set period of time (usually a few seconds).[31] Of course, like everything else on the Internet, Snapchat messages have a way of not actually disappearing. There exist several workarounds that allow recipients to save images.[32]

Yik Yak is a social media app targeted to college students that allows users to share their thoughts and keep their privacy.[33] The key feature is that the app allows for (and markets itself on) anonymous posting. Users enter into the app whatever random thoughts or observations they may have and the app provides the world "a feed of all the . . . things people are saying around you."[34]

B. THREATS AND INTIMIDATION ARE COMMONPLACE ON SOCIAL MEDIA

On December 15, 2015, the Los Angeles Unified School District (LAUSD), the second largest school district in the nation, abruptly closed its doors in response to an electronic threat received over email.[35] Coming on the heels of a terrorist attack in neighboring San Bernardino, some observers felt that LAUSD acted prudently.[36] The anonymous threat, which was ultimately deemed a hoax by district officials, displaced 640,000 students and shut down 900 campuses, as well as 187 charter schools.[37] In the end, the hoax achieved exactly what it set out to do—to stoke fear and generate massive disruption.

What happened in Los Angeles, regrettably, was not an isolated incident. Social media, and other electronic communication forms (*e.g.*, emails, texts), has opened new avenues for perpetrators to threaten and intimidate.[38] No longer does someone need to physically stalk their prey to deliver a message; they can now threaten *anyone*, *anywhere* with just one click of their cell phone. And because the threatening communications are often

---

14, 2015), http://www.wsj.com/articles/what-celebrities-can-teach-companies-about-social-media-1444788220.

31. Larry Magld, *What Is Snapchat and Why Do Kids Love It and Parents Fear It?*, FORBES (May 1, 2013), http://www.forbes.com/sites/larrymagid/2013/05/01/what-is-snapchat-and-why-do-kids-love-it-and-parents-fear-it/.

32. *Id.*

33. YIK YAK, http://www.yikyak.com/home (last visited Jan. 26, 2016).

34. *Id.*

35. Tamara Audi et al., *Los Angeles Officials Defend Decision to Close Schools After Threat*, THE WALL STREET JOURNAL (Dec. 16, 2015), http://www.wsj.com/articles/los-angeles-schools-closed-after-threat-1450193499.

36. *See id.*

37. *Id.*

38. *See* L. B. Lidsky, et al., *Incendiary Speech and Social Media*, 44 TEX. TECH. L. REV. 147, 148-49 (2011).

prepared in private and can be delivered anonymously, they are not regulated by social norms that would harshly condemn such behavior.[39] Thus, it should come as little surprise that threats are increasing every year and online threats are fueling that growth.

A 2015 study conducted by the National School Safety and Security Services found that the act of calling in a bomb threat has become a thing of the past—37% of threats studied "were sent electronically, using social media, email, text messaging and other online resources. Social media threats, alone, account for 231 threats (28%)."[40] Cyberstalking is also on the rise, with perpetrators turning to social media to announce what harm they intend to do to their victims.[41] Further, "apps like Yik Yak, After School and Whisper are creating special problems for investigators because [culprits] can post anonymously, making it harder to track down offenders."[42] And when the *Elonis* decision is added to the calculus—which has made a federal prosecutor's job more difficult by requiring a higher level of culpability before a conviction can be attained—policing and successfully prosecuting online threats can be a difficult road to travel.

III. THE GUILTY MIND: WRONGDOING MUST BE CONSCIOUS TO BE CRIMINAL

In *Elonis*, Chief Justice Roberts observed "that a defendant must be 'blameworthy in mind' before he can be found guilty."[43] For the Court, convicting Elonis for mere negligence under a "reasonable person" standard was at odds with "the conventional requirement for criminal conduct—*awareness* of some wrongdoing."[44] Indeed, at common law it was well recognized that "an unwarrantable act without a vicious will is no crime at all."[45] Historically, this distinction served to "protect the morally innocent from unjust punishment."[46] Today, our criminal jurisprudence embraces a

---

39. *Id.* at 149.

40. Ken Trump, *Study Finds Rapid Escalation of Violent School Threats*, NAT'L. SCH. SAFETY AND SEC. SERV. (Feb. 9, 2015), http://www.schoolsecurity.org/2015/02/study-finds-rapid-escalation-violent-school-threats/.

41. *See* Andrew King-Ries, *Teens, Technology, and Cyberstalking: The Domestic Violence Wave of the Future?*, 20 TEX. J. WOMEN & L. 131 (2011).

42. Trump, *supra* note 40.

43. Elonis v. United States, 135 S.Ct. 2001, 2009 (2015).

44. *Id.* at 2011.

45. 4 WILLIAM BLACKSTONE, COMMENTARIES *21; *see also* Morissette v. United States, 342 U.S. 246, 251 (1952).

46. Ann Hopkins, *Mens Rea And The Right To Trial By Jury*, 76 CAL. L. REV. 391, 391 (1988).

"guilty mind" principal and generally requires that "wrongdoing must be conscious to be criminal."[47] As the Supreme Court has recognized:

> The contention that an injury can amount to a crime only when inflicted by intention is no provincial or transient notion. It is as universal and persistent in mature systems of law as belief in freedom of the human will and a consequent ability and duty of the normal individual to choose between good and evil. A relation between some mental element and punishment for a harmful act is almost as instinctive as the child's familiar exculpatory "But I didn't mean to," and has afforded the rational basis for a tardy and unfinished substitution of deterrence and reformation in place of retaliation and vengeance as the motivation for public prosecution.[48]

To this end, there are two central elements of every crime: the *actus reus*, or the commission (or omission) of some act prohibited by law; and the *mens rea*, or some criminal state of mind.[49] The concern of criminal law is with the level of intentionality with which the defendant acted, in other words, with what the defendant intended, knew, or should have known when he acted.[50]

Yet, even though at common law a defendant's mental state was paramount, for much of American legal history there lacked clear and consistent standards of moral criminal culpability.[51] In 1952, in *Morissette v. United States*, the Supreme Court observed that the then-current state of the law was far from clear on criminal culpability standards, noting that the legal landscape was defined by the "variety, disparity and confusion of [judicial] definitions of the requisite but elusive mental element."[52] In response, the drafters of the Model Penal Code developed five defined levels of criminal culpability, which many states have now largely adopted in

---

47. *See Morissette*, 342 U.S. at 252; *Elonis*, 135 S.Ct. at 2009.

48. *Morissette*, 342 U.S. at 251-52.

49. *See* 1 WAYNE LAFAVE, SUBSTANTIVE CRIMINAL LAW § 5.1 (2d ed. 2003).

50. *See id.*

51. Paul H. Robinson, *A Brief History of Distinctions in Criminal Culpability*, 31 HASTINGS L.J. 815, 815 n. 3 (1979) ("As a result of their pioneering endeavor, the Model Penal Code drafters reduced nearly eighty miscellaneous culpability terms to five carefully defined levels.") ("There were no previous formulations of this nature.").

52. *Morissette*, 342 U.S. at 252.

whole or in part.[53] They are, in order of most conscious and culpable: "purposely," "knowingly," "recklessly," "negligently," and "faultlessly" (absolute liability).[54]

Model Penal Code section 2.02 sets forth the "General Requirements of Culpability."[55] In response to *Elonis*, this paper considers the first three culpable states. A person acts "purposely" if he has an actual intention to do the particular kind of harm that in fact was done.[56] A person acts "knowingly" if he has an awareness of conduct or consequences and knows to a practical certainty that the result will follow from a certain act.[57] A person acts "recklessly" if he "disregards a substantial and unjustifiable risk that the material element [of the offense] exists or will result from his conduct."[58] In other words, the person foresees that harm might occur but does the act anyway.

IV. A ROADMAP TO PROVING INTENT FOR SOCIAL MEDIA THREATS

Proving a perpetrator's intent to threaten is inherently difficult. As Justice Ginsburg recognized, "[h]ow does one prove what's in somebody else's mind?"[59] And yet a criminal prosecutor *is* tasked with proving exactly what was in the defendant's mind at the moment he logged on to social media and posted the threatening communication at issue. In some cases, a defendant will admit during a police interrogation that he intended to intimidate the victim.[60] Direct evidence, however, is the exception.[61] In most cases a defendant will deny a malicious intent and likely that he even authored the threatening message.[62] Thus, proof of criminal intent most often

---

53. Robinson, *supra* note 51, at 815; *see, e.g.*, 720 ILL. COMP. STAT. 5/4-4 (2012); N.J. STAT. ANN. § 2C:2-2 (West 2016); N.Y. PENAL LAW § 15.05 (McKinney 2016); 18 PA. STAT. AND CONS. STAT. ANN. § 302 (West 2016); TEX. PENAL CODE Ann. § 6.03 (West 2015); WASH. REV. CODE ANN. § 9A.08.010 (West 2009).

54. MODEL PENAL CODE § 2.02.

55. *Id.*

56. *Id.* § 2.02(2)(a).

57. *Id.* § 2.02(2)(b).

58. *Id.* § 2.02(2)(c).

59. Transcript of Oral Argument, *supra* note 14, at 4.

60. *See* Judy Harrison, *Man Who Stalked Woman Studying in Maine Sentenced to 2 Years*, BANGOR DAILY NEWS (Feb. 10, 2016), http://bangordailynews.com/2016/02/10/news/portland/man-who-stalked-woman-studying-in-maine-sentenced-to-2-years/.

61. 1 WITKIN, CAL. CRIM. LAW, Elements, § 3, at 261 (4th ed. 2012).

62. *See id.* at 56 ("However, while the defendant may testify to his or her own lack of criminal intent [citation], it is rare that direct evidence of criminal intent is available to the prosecution").

turns on circumstantial evidence—on piecing together a diverse set of facts to prove to the jury what drove the defendant's actions.[63]

Generally, the fact finder in a civil trial may base her findings on a preponderance of the evidence.[64] In criminal trials, however, the defendant is presumed innocent.[65] To convict, a prosecutor must prove that the defendant is guilty beyond a reasonable doubt.[66] In other words, that guilt is the only reasonable interpretation of the evidence. This is a daunting task.

A. IDENTIFYING AN ANONYMOUS POSTER

The first step for police investigators and prosecutors may well be identifying the actual perpetrator—the source of the threatening communication. As discussed *supra*, many forms of electronic communication allow for, and encourage, anonymous posting.[67] In the civil context, because the First Amendment ensures the right to engage in anonymous speech,[68] unmasking an anonymous poster generally requires that the petitioner (1) make an effort to notify the anonymous poster that the subpoena or motion for disclosure is going to be filed, (2) allege a facially valid cause of action and produce *prima facie* evidence to support all of the elements of the cause of action within her control, and (3) demonstrate that the information being sought is necessary to identify the defendant and that the defendant's identity is relevant to the plaintiff's case.[69]

In the criminal context, the Fourth Amendment's prohibition on warrantless searches and seizures is triggered.[70] The Federal Electronic Communications Privacy Act (ECPA) authorizes the government to access stored communications and transaction records held by third-party service providers.[71] States have similar statutes regulating law enforcement's ability to seize electronic data.[72] To obtain the identifying information from service

---

63. *Id.*

64. *See, e.g.*, CAL. EVIDENCE CODE § 115 ("Except as otherwise provided by law, the burden of proof requires proof by a preponderance of the evidence.").

65. *See, e.g.*, JUDICIAL COUNCIL OF CALIFORNIA CRIMINAL JURY INSTRUCTIONS, CALCRIM No. 220 (2015); CAL. PENAL CODE § 1096 (West 2015).

66. *Id.*

67. *See supra* Part II.

68. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

69. *See, e.g.*, SaleHoo Grp., Ltd. v. ABC Co., 722 F. Supp. 2d 1210, 1215-16 (W.D. Wash. 2010); Sony Music Entm't Inc. v. Does 1-40, 326 F. Supp. 2d 556, 564-65 (S.D.N.Y. 2004).

70. *See, e.g.*, *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 132 (E.D. Va. 2011); U.S. v. Perrine, 518 F.3d 1196, 1201-05 (10th Cir. 2008).

71. 18 U.S.C. § 2703 (2012).

72. *See, e.g.*, California Electronic Communication Privacy Act, (effective January 1, 2016).

providers, the government must offer "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation."[73] The ECPA has survived constitutional challenge, as courts have consistently held that Internet users have "no Fourth Amendment privacy expectation in the subscriber information" they give to their Internet service providers.[74] Nor do they have an expectation of privacy in their IP address when they send that information voluntarily to websites and web services.[75] As such, unmasking an anonymous online speaker can be accomplished in short order if law enforcement officers are able to marshal the appropriate facts in support of the government's application seeking a court order for disclosure.

Identifying the digital source of a communication does not signal the end of a criminal investigation, however. In most cases, it is just the beginning of the fact gathering needed for a successful prosecution. Remember, a prosecutor must prove that the defendant authored the threatening message. Even when the message comes from a social media account clearly associated with the defendant, he may still deny authoring the statement. Accordingly, a prosecutor will need to present other evidence, both direct and circumstantial, to prove authorship. For instance, a search of the defendant's electronic devices may indicate whether they were used to prepare the statement. Authorship can also be proved by demonstrating that the defendant was the only individual with access to the relevant passwords for his social media platforms or electronic devices. And proof that he authored other online communications close in time to the message at issue would demonstrate that he had control over his social media platforms at the relevant time, affording him with the opportunity to make the threatening communication.

Interviews of family and friends can reveal additional evidence of authorship. Despite denying criminal culpability during police interrogation, the defendant may have made earlier admissions to those people close to him. Additionally, family and friends may verify that the defendant's speech pattern—either historical or recently adopted—matches the language of the electronic threat, further corroborating his role in drafting. Finally, those witnesses might possess evidence of motive: for example, a preexisting conflict with the target of the threat.

---

73. 18 U.S.C. § 2703(d) (2012).

74. U.S. v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008).

75. *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 132 (E.D. Va. 2011).

B. KEY EVIDENCE TO ESTABLISHING CULPABILITY

Of course, proving that the defendant authored the threat is only part of the burden the prosecutor must meet at trial. She must additionally prove that the perpetrator acted with either the purpose of issuing a threat or with knowledge that the communication would be viewed as a threat. The message at issue itself, therefore, can serve as an important piece of evidence in determining culpability. For example, threats that identify a specific person or location as their target and are authored using a social media platform the writer knows will reach his target (thus placing the target in fear) are more likely to have been intended as genuine threats. By contrast, a nonspecific threat which names no particular target (*e.g.*, "Someday, I am gonna shoot up a school") may rightly cause a police agency to investigate, but the words of the threat themselves do little to prove a specific intent that the communication be taken as a threat.

The issue is further complicated for prosecutors when we consider the fact that discerning a speaker's subjective intent is particularly difficult based on just an electronic communication. For instance, what is the tone? The message lacks key contextual clues and associated nonverbal communication present in face-to-face interaction. After all, body language and facial expressions cannot be judged by reading words on a screen.

Law enforcement can attempt to overcome this evidentiary hurdle by asking the victim (or other third parties) for assistance in making pretextual calls that would elicit a confession from the accused on the ultimate questions of authorship and intent. These surreptitiously recorded conversations might secure unguarded admissions. Jurors would ultimately be able to hear for themselves the defendant's tone and demeanor as he speaks about the threatening message in question.

The circumstances under which the message was authored may also shed light into the author's intent. What was the defendant's relationship with the victim? Was there already a pattern of threatening behavior? Was he under pressure at home or at work? Answering these questions could shed light into his mental state. Although electronic communications are often drafted in private, there may be a witness (such as a friend or family member, as discussed *supra*) who is aware of the defendant's personal situation, perhaps participated in drafting the message, or was later informed by the defendant about the message and its intent.

Other social media postings and communications contemporaneous to the threatening message at issue can further illuminate intent. Do they show a pattern of abuse toward other people? When sarcasm or humor is used, is it obvious? Are emoticons used in other communications to soften tone, but are absent in the message at issue?

A search of the defendant's home and belongings can also be revealing. Did the police discover any physical evidence that would demonstrate

his ability to carry out his threat? For instance, if the threat discusses the use of specific weapons, were they found in his possession? Finding the instruments to carry out his threat in his custody would tend to demonstrate that his intent to threaten, and indeed gravely harm, were genuine.

Finally, although "[e]vidence of a crime, wrong, or other act is not admissible to prove a person's character in order to show that on a particular occasion the person acted in accordance with the character,"[76] Federal Rules of Evidence 404(b)(2) does allow the admission of such character evidence to prove a defendant's "intent."[77] Thus, with appropriate notice given to the defendant,[78] evidence that on a prior occasion the defendant had threatened the victim (or other individuals) can be introduced to demonstrate that it was his intent to do so on the occasion at issue. Of course, Rule 404(b)(2) must be balanced with Rule 403, which allows the court to exclude otherwise relevant and admissible evidence "if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence."[79]

V. EXERCISING PROSECUTORIAL DISCRETION ON SOCIAL MEDIA THREATS

For many advocates, the *Elonis* decision wrongly protects perpetrators over their victims.[80] Shifting criminal culpability away from what a reasonable person would find threatening and moving it toward requiring proof that the defendant intended to intimidate may very well fail to address the harm, threats, and intimidation inflicted—namely, the fear of violence and the psychological, emotional, and physical disruption it causes.[81] The harm a threat inflicts does not depend on the speaker's sincerity. On the other hand, prosecuting a speaker for speech that might be reasonably interpreted as threatening, especially when that was not the speaker's intent, could chill speech and inhibit the free trade in ideas. As the Supreme Court has recog-

76. FED. R. EVID. 404(b)(1).

77. *Id.* at 404(b)(2).

78. *Id*. at 404(b)(2)(A)-(B) ("On request by a defendant in a criminal case, the prosecutor must: (A) provide reasonable notice of the general nature of any such evidence that the prosecutor intends to offer at trial; and (B) do so before trial—or during trial if the court, for good cause, excuses lack of pretrial notice.").

79. FED. R. EVID. 403.

80. *See, e.g.*, Brief for the Nat'l Network to End Domestic Violence as Amici Curiae Supporting Respondent, Elonis v. United States, 135 S. Ct. 2001 (2015) (No. 13-983).

81. *See* Virginia v. Black, 538 U.S. 343, 360 (2003) (quoting R.A.V. v. City of St. Paul, Minn., 505 U.S. 377, 388 (1992)) ("a prohibition on true threats 'protect[s] individuals from the fear of violence' and 'from the disruption that fear engenders,' in addition to protecting people 'from the possibility that the threatened violence will occur.'").

nized, "[i]f there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[82]

For prosecutors, charging perpetrators for social media threats presents challenges that are new to the prosecutorial profession. Prosecutors are tasked with determining whether a threat is credible. But they must also determine context in a contemporary medium which lacks traditional social cues. Failure to properly identify and assess a threat can lead to tragic consequences.[83] Overreaction, however, can lead to public ridicule, or worse—creating an injustice by charging a person for conduct that is not a crime.[84] How should prosecutors therefore exercise discretion in bringing cases?

Governmental entities have begun grappling with the inherent tension between public safety and a robust public discourse.[85] The line becomes more difficult to draw when many of the alleged perpetrators are children, like the teenage online gamer arrested for making threats in Texas, who often lack the maturity to consistently exhibit good judgment.[86] There should be no disagreement that law enforcement should investigate all potentially credible threats. But, once police have completed their investigation, prosecutors must then determine whether it is appropriate to charge someone for online threats. In this process, prosecutors must be mindful of their obligation to be fair and just.[87] Below we propose guidelines for prosecutors to consider when making this determination.

A. GENERAL CRITERIA CONSIDERED IN CHARGING THE ACCUSED

The primary responsibility of a prosecutor in charging is to determine whether or not there is sufficient evidence to convict the accused of the particular crime in question and to authorize the filing of appropriate charges.[88] Prosecutors should never charge a person with a crime because of pub-

---

82. Texas v. Johnson, 491 U.S. 397, 414 (1989).

83. *See* Adam Nagourney, Michael Cieply, Alan Feuer, & Ian Lovett, *Before Brief, Deadly Spree, Trouble Since Age 8*, N.Y. TIMES (June 1, 2014), http://www.nytimes.com/2014/06/02/us/elliot-rodger-killings-in-california-followed-years-of-withdrawal.html?_r=0 (chronicling the disconcerting online behavior of mass murderer Elliot Rodger and the fact that no one alerted the police before his deadly spree).

84. *See* Jeff Yang, *Did Los Angeles Overreact to School Threat?*, CNN (Dec. 15, 2015),http://www.cnn.com/2015/12/15/opinions/yang-los-angeles-schools-threat/index.html; Malisow, *supra* note 5.

85. *See, e.g.*, *Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media*, THE CROWN PROSECUTION SERV., http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media#accept (last visited Jan. 24, 2016).

86. Gross, *supra* note 3.

87. Berger v. United States, 295 U.S. 78, 88 (1935).

88. *See* CAL. STATE BAR RULES OF PROF'L CONDUCT R. 5-110.

lic pressure or for political favor. In practice, a prosecutor should charge if the following basic requirements are satisfied: (1) based on a complete investigation and a thorough consideration of all pertinent data readily available, the prosecutor is satisfied that the evidence shows the accused is guilty of the crime to be charged; (2) there is legally sufficient, admissible evidence of a crime; (3) there is legally sufficient, admissible evidence of the accused's identity as the perpetrator of the crime charged; and (4) the prosecutor has considered the probability of conviction by an objective fact-finder hearing the admissible evidence.[89]

B. SPECIFIC CRITERIA CONSIDERED IN CHARGING SOCIAL MEDIA THREATS

1. Sufficiency of the Evidence Regarding Accused's Intent

Charging a social media threat requires that prosecutors carefully examine the evidence of intent. Does the available direct and circumstantial evidence prove that the author's goal was to instill fear in the recipient of the communication? The possibility of an innocent explanation for the online post should be fully resolved before filing a criminal complaint. Consequently, prosecutors should answer two critical questions before charging these types of cases:

> (1) Is the theory of guilt supported by the evidence?
>
> (2) Is there any reasonable theory of innocence (whether or not advanced by the suspect) that is consistent with our evidence?

If the answer to the second question is affirmative, prosecutors should resolve that theory of innocence within the filing stage of the case. Specifically, they should be able to identify credible evidence that refutes the innocence theory. This requires prosecutors to think slightly differently when they screen potential online threat cases. Prosecutors usually focus their crime charging analysis on the evidence that proves guilt, rather than evidence that disproves a yet unarticulated defense theory. But, in the online threat context, prosecutors would be well served to also consider evidence which disproves potential theories of innocence.

---

89. NAT'L PROSECUTION STANDARDS, Part IV, § 4-1.3 & 4-2.4 (NAT'L DIST. ATTORNEYS ASS'N 2009).

2. Current Status of the Online Threat

Actions taken by the suspect after the post (and before contact by law enforcement) may be relevant to the crime-charging decision. For example, if the author quickly removed the message from his social media account and offered an apology for any unintended harm caused, these actions may show that the author did not intend for the message to be understood as a threat. It would also tend to corroborate any later claims that the message was intended as sarcasm or a badly conceived joke.

Of course, efforts by a suspect to destroy evidence of his offense should not be confused with proof of innocence. Perpetrators of crime who fear that police have been contacted often take steps to destroy evidence of their guilt, such as removing threatening posts so that law enforcement cannot capture screen shots and use them as evidence.

3. The Age and Maturity of the Accused

Prosecutors should take extra care when charging juveniles for online threats. Indeed, there is consensus across the country that juveniles who commit crime should be handled differently than adults by the criminal justice system.[90] State legislatures and the law enforcement community understand that juveniles' judgment and reasoning abilities are not yet developed to the same extent as adults'.[91] Accordingly, many state juvenile justice systems are built around a restorative justice model, which focuses on the needs of the offender, instead of simply punishment.[92] Under this approach to justice, juvenile offenders are encouraged to take responsibility for their actions and to repair the harm they have done by taking proactive measures, such as apologizing to their victims, returning stolen property, and providing community service. Restorative justice provides help for the offender in order to avoid future offenses.

Restorative justice's focus on the juvenile offender underscores the fact that not every online threat committed by a minor should necessarily be charged and prosecuted in a similar fashion. Consequently, when the perpetrator of an online threat is a juvenile, prosecutors should consider and balance two additional factors: (1) the seriousness of the threat and (2) the amount of juvenile justice intervention required. In regards to seriousness of the threat, we suggest that prosecutors weigh issues like: What is the

---

90. *Child Welfare and Juvenile Justice*, GPSOLO MAGAZINE, April/May 2008, Volume 25, Number 3, http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/restoringjuvenilejustice.html.

91. *Id.*

92. *See, e.g.*, CAL. WELF. & INST. CODE § 202.

nature of the threat that was delivered? Does the available evidence prove that the minor clearly understood that his message would be interpreted as a threat? Does the evidence suggest that the minor planned to carry out the threat, or was the message an effort to gain attention, for example, by disrupting activity at his school campus?

Once a prosecutor has gained an understanding of the issues surrounding the seriousness of the offense, she should determine the level of juvenile justice intervention that is required to ensure that the minor appreciates the harm he caused and to help ensure that he does not reoffend. It should be noted that juvenile prosecutors have a broad range of consequences they can seek for delinquent behavior by minors. For example, a prosecutor may opt not to file a juvenile case and instead seek informal diversion that does not result in custody or a juvenile court adjudication.[93] Such diversion may include juvenile probation supervision, mandated counseling, and efforts to repair the harm caused by engaging in positive community service. On the other end of the spectrum, state law may permit a prosecutor to seek prosecution in adult court.

Before deciding what consequences to seek, prosecutors should weigh issues like: Did the minor appear to be genuinely remorseful during the police investigation? Are the parents/guardians of the minor fully involved in his life and are they willing to cooperate with the juvenile justice system in imposing consequences for this crime and closely supervising the minor? Does the minor have any prior juvenile offenses, and how successful were previous attempts by the juvenile court to rehabilitate the minor? This determination should drive the ultimate crime-charging decision.[94]

4. Likelihood of Re-offense

An ultimate goal of criminal prosecution is to provide a deterrent effect for the accused in order to prevent future offenses. Consequently, likelihood of re-offense is the final issue prosecutors should consider before making the charging decision. This is a question that requires prosecutors to assess the suspect holistically in order to assess if he poses a significant recidivism threat. Factors to consider include: What was the defendant's level of involvement in composing and delivering the threat at issue? How sophisticated was his criminal activity? Did he admit guilt in the offense, recognize the harm caused, and accept responsibility? Does the suspect have a criminal history, including a history of re-offense while under court supervision (*e.g.*, probation)? What is the recommendation of the police investigators? Answering these questions will assist the prosecutor in de-

93. *Id.* at § 654.
94. *See* NAT'L PROSECUTION STANDARDS, Part IV, § 4-11.6.

termining the severity of charges to impose. Certainly, suspects likely to re-offend should be charged and prosecuted more aggressively, because those individuals pose the greatest risk to the community.

VI. RECKLESSNESS IN THE AGE OF SOCIAL MEDIA

In his *Elonis* concurrence, Justice Alito laments that "[a]ttorneys and judges need to know which mental state is required for conviction under 18 U.S.C. §875(c), an important criminal statute. . . . But the Court refuses to explain what type of intent was necessary."[95] Undaunted, the Justice proceeds to answer the ultimate question left open. As an initial matter, he agrees with the majority that section 875(c) requires a higher *mens rea* culpability level than negligence.[96] One step above negligence on the hierarchy of criminal culpability lies recklessness. For the Justice, recklessness is the appropriate mental state. "[W]hen Congress does not specify a *mens rea* in a criminal statute, we have no justification for inferring that anything more than recklessness is needed."[97] Overreaching and imposing a "purposely" or "knowingly" standard would cross "over the line that separates interpretation from amendment."[98] And besides, for the Justice, recklessness is sufficient: "Someone who acts recklessly with respect to conveying a threat necessarily grasps that he is not engaged in innocent conduct. He is not merely careless. He is aware that others could regard his statements as a threat, but he delivers them anyway."[99]

As for Elonis's First Amendment concerns, Justice Alito deftly dispatches with them. As an initial matter, the Justice rightly observes that "[t]rue threats inflict great harm and have little if any social value."[100] The argument that threatening language made without the intent to threaten may be either "therapeutic" or "artistic" completely fails to appreciate that "whether or not the person making a threat intends to cause harm, the damage is the same."[101] On balance, for the Justice, "the fact that making a threat may have a therapeutic or cathartic effect for the speaker is not sufficient to justify constitutional protection."[102] Justice Alito then addresses the concern that a recklessness standard would chill speech by penalizing

---

95. Elonis v. United States, 135 S.Ct 2001, 2013-14 (2015) (Alito, J., concurring in part and dissenting in part).

96. *Id.* at 2014-15 (Alito, J., concurring in part and dissenting in part).

97. *Id.* at 2015 (Alito, J., concurring in part and dissenting in part).

98. *Id.* (Alito, J., concurring in part and dissenting in part)

99. *Id*. (Alito, J., concurring in part and dissenting in part)

100. Elonis v. United States, 135 S.Ct 2001, 2016 (2015) (Alito, J., concurring in part and dissenting in part).

101. *Id.* (Alito, J., concurring in part and dissenting in part)

102. *Id.* (Alito, J., concurring in part and dissenting in part)

"statements that may be literally threatening but are plainly not meant to be taken seriously."[103] Analogizing to the Court's libel jurisprudence, Justice Alito argues that the freedom of speech is amply protected when the law requires proof that threatening statements were made with reckless disregard as to their threatening nature.[104]

Assuming *arguendo*, that Justice Alito's analysis is correct—that the statute compels a recklessness standard and that the First Amendment condones it—on a policy level, is recklessness appropriate? Does it actually remove dangerous people from the community and deter other criminal behavior? Does it take into consideration the unique nature of online communications? Or does it cast too broad of a net, ensnaring innocent behavior?

A person acts "recklessly" if he "disregards a substantial and unjustifiable risk that" his communication is threatening or that someone may be threatened by his words.[105] Context matters under this standard. Unlike the reasonable person standard, which simply asks whether someone reasonable would consider the message threatening, the recklessness standard gets into the mind of the speaker and requires a prosecutor to demonstrate that the speaker was aware that his words could be viewed as threatening and that he, nonetheless, transmitted the communication in spite of it.[106]

But consider the declarant who is speaking with a friend online and genuinely believes that his statement "I am going to kill you tomorrow at school" will be taken as a joke. He does not consciously foresee that harm might occur if a third party later reads a portion of that exchange. Yet, as discussed *supra*, the online communication itself conveys neither tone nor intent. Read by someone in isolation (such as in a screenshot or printout)[107] it may seem credible. In legislating the appropriate mental state for the crime of transmitting threats online, who should bear the risk that this communication may inflict harm—the speaker at the expense of free speech or the recipient at the expense of public safety?

It can be argued that the declarant is reckless and, thus, should be held criminally liable, because he knows by experience that online communications lack tone and that his communication may be misinterpreted. Indeed,

---

103. *Id.* at 2017(Alito, J., concurring in part and dissenting in part).

104. *Id.* at 2017 (Alito, J., concurring in part and dissenting in part) (citing Garrison v. Louisiana, 379 U.S. 64, 75 (1964) (criminal libel); New York Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964) (civil libel)).

105. *See* MODEL PENAL CODE § 2.02(2)(c).

106. *See id*. § 2.02(2)(c), (d); *Elonis*, 135 S.Ct at 2008, 2015 (Alito, J., concurring in part and dissenting in part).

107. *See* Malisow, *supra* note 6 (noting that in charging a teenager for making terroristic threats, which carries a penalty of two to ten years in state prison, "[p]rosecutors say they don't have the entire thread—instead, they have three comments on a cell-phone screenshot.").

people who lack the appropriate context repeatedly misinterpret online communications as threats.[108] Thus, he ignored a "substantial" and, arguably, "unjustifiable risk" that someone could be threatened. Instead, if he meant it as a joke, the complete message could have read "I am going to kill you at school. *Just kidding!*"; thus, minimizing the risk for confusion.

Or should the recipient bear the risk? After all, social media allows for the distribution of communications to far wider audiences than the speaker can fairly anticipate. A private message can be shared, retweeted, snapped, and reposted within seconds and quickly spread virally, and all without the speaker's consent.[109] A communication meant as a joke between two friends can become a deranged threat to kill children that a person thousands of miles away, in another country no less, finds credible. People's sense of what is threatening has yet to catch up with technology. They fail to appreciate their lack of context and do not have the sense to seek it out. Just because words can be misconstrued online does not mean that the default position should be that the speaker is punished for someone else's misinterpretation.

In the end, the recklessness standard in today's reality of constant unfiltered online communication would at best chill speech (if the speakers were even aware that sarcasm had been elevated to a federal offense); at worst, it would wrongly prosecute and convict citizens exercising their freedom of speech. More troubling, the standard would enable and embolden prosecutors to charge and prosecute innocent, if perhaps careless, speakers under the lesser culpability standard. On balance, the better rule to protect speech and public safety would be to require proof that the defendant *purposely* issued a threat or did so with the *knowledge* that his communication would be viewed as a threat. True credible threats of violence, like those at issue in *Elonis*, can be successfully prosecuted under the heightened culpability standards. Recklessness is unnecessary to deter criminal behavior or remove dangerous people from social media. Instead, it has the potential to sweep in innocent, but careless, speech. In so doing, the recklessness standard fails to elevate moral culpability above negligence.[110] The

---

108. *See, e.g.*, Malisow, *supra* note 6; Tracy Bloom, *Apparent 'Practical Joke' Threat Posted to Social Media Leads to Arrest of Another Santa Clarita Valley Teen*, KTLA (Aug. 8, 2014), http://ktla.com/2014/08/18/apparent-practical-joke-threat-posted-to-social-media-leads-to-arrest-of-another-santa-clarita-valley-teen/.

109. *See id.*

110. *See* Kenneth W. Simons, *Culpability and Retributive Theory: The Problem of Criminal Negligence*, 1994 J. CONTEMP. LEGAL ISSUES 365, 374 (1994) (examining the level of abstraction—subjective or objective—at which the recklessness inquiry implicates an actor's personal awareness of a known risk); Kenneth W. Simons, *Rethinking Mental States*, 72 B.U. L. REV. 463, 470 (1992) (noting the miniscule effective difference between negligence and recklessness under the Model Penal Code); see 1 WAYNE R. LAFAVE, SUBSTANTIVE CRIM.INAL LAW § 5.4 (2d ed., Thomson West 2003), for a discussion of the

accused is still being tried and convicted for "an unwarrantable act without a vicious will."[111]

VII. CONCLUSION

Threats, whether made online or in person, cause tremendous harm and disruption. Although this paper argues recklessness is inappropriate for online threats, it is not to diminish the effect these crimes have on their victims. Law enforcement should investigate every potential threat, whether made online or otherwise. And when a threat is found to be genuine, proving up purpose or knowledge through evidence can be accomplished through a variety of techniques, as discussed herein. However, because of the unique nature of social media and its ability to widely and indiscriminately disseminate idiosyncratic messages, a recklessness standard has the unjustified danger of punishing free speech without increasing public safety.

---

practical distinctions between criminal negligence and recklessness. *See also* Matthew R. Ginther et. al., *The Language of Mens Rea*, 67 VAND. L. REV. 1327, 1330 (2014) (summarizing empirical findings demonstrating the difficulty that jurors have in assessing the capability level of recklessness).

111. King-Ries, *supra* note 41.