Comments

Trolling Attacks and the Need for New Approaches to Privacy Torts

By ARTHUR GAUS*

Introduction

ANONYMITY DEFINES THE INTERNET. On the Internet, users can share information and ideas, engage in commercial transactions, and debate relevant issues without ever having to reveal their true identities. Anonymity, however, comes with lowered inhibitions. Without the threat of a blot on one's good name, Internet users operate unencumbered by generally accepted social norms and, as a result, are more prone to say and do things that they perhaps would not under their real identities. Benefits certainly do exist: The anonymity of the Internet has promoted a freer exchange of ideas and a more diverse online economy.[1] Anonymity in general, however, erodes accountability. The Internet's diminished capacity for accountability has bred small but powerful communities of Internet "trolls."[2] The conduct of these communities and the individuals affiliated with them is extremely varied; it ranges from benign contrarian behavior on online message boards to the destructive circulation of intentionally harmful Internet memes.[3] This paper will demonstrate that our current legal

* J.D., University of San Francisco School of Law (2012); B.A. University of California, Santa Cruz.

1. Zizi Papacharissi, *The Virtual Sphere: The Internet as a Public Sphere*, 4 NEW MEDIA & SOC'Y 9, 26 (2002), *available at* http://tigger.uic.edu/~zizi%20/Site/Research_files/VirtualSphere.pdf.

2. Defined *infra* Part I.A, "trolls" refers generally to Internet users who engage in a broad spectrum of intentionally mischievous behavior designed to illicit strong reactions from the targets of their activities. *See* Ana Marie Cox, *Making Mischief on the Web*, TIME (Dec. 16, 2006), http://www.time.com/time/magazine/article/0,9171,1570701,00.html.

3. "Meme" is a neologism of the Internet, defined as "an image, video, piece of text, etc., typically humorous in nature, that is copied and spread rapidly by Internet users, often with slight variations." *Meme Definition*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/english/meme (last visited Nov. 16, 2012).

infrastructure—designed without the harms of the online world in mind—is unsuited to handle the most harmful and insidious forms of Internet "trolling." In response, it will propose an updated tort regime to compensate the victims of this behavior and deter future attacks.

I. The Basics of Trolling

A. What is Trolling, Generally?

A wide variety of behavior falls under the umbrella of online trolling, and it produces a wide spectrum of harms. On the less harmful end of the spectrum are intentionally provocative postings to message boards, sometimes referred to as "concern trolling."[4] This behavior generally involves anonymously posting intentionally contrarian or sometimes shocking ideas to disrupt online debates.[5] This form of trolling warrants no regulatory effort because the harms are negligible. Even the most pernicious forms of "concern trolling" harm only the integrity of the online community attacked and generally can be addressed through careful self-moderation of the offended forums.[6]

B. Lulz Trolling

On the other end of the spectrum are the trolling attacks that require new regulation. The most harmful forms of trolling, the forms with which this paper is most concerned, are often classified under the umbrella of "cyberbullying" or "cyberharassment."[7] Broadly defined, cyberbullying refers to malicious online behavior where both the perpetrator and the target are minors.[8] By contrast, cyberharassment refers to malicious behavior where one or both parties are adults.[9] These forms are distinguishable from more benign trolling behaviors in that they frequently involve elements of what Nancy Kim has described as "cyberdeception" or "online insults" and usually involve the use of images.[10] Also, the targets of these attacks are frequently not acquainted with the perpetrators outside of the context of the attack.[11]

4. Cox, *supra* note 2.
5. *Id.*
6. *See id.*
7. Nancy S. Kim, *Web Proprietorship and Online Harassment*, 3 UTAH L. REV. 993, 995–96 (2009).
8. *What is Cyberbullying Exactly?*, STOPCYBERBULLYING, http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html (last visited Nov. 6, 2012).
9. *Id.*
10. Kim, *supra* note 7.
11. *Id.* at 1009.

A wide variety of online behaviors produce these trolling attacks. For example, a notorious cyberdeception case involved an anonymous Craigslist user posting a phony solicitation for sex on Craigslist.[12] The advertisement encouraged viewers to respond with highly explicit responses and photographs.[13] The author of the advertisement then published all the responses, including photos, personal e-mails and phone numbers on a popular website for the trolling community.[14] From there, the personal information and photographs of those who responded to the ad were disseminated to the Internet at large.[15] People associated with the ad suffered real consequences—some lost jobs, some lost marriages, and all had their reputations viciously sullied.[16]

Another trolling attack that fits the category of cyberdeception involved the "Megan Had It Coming" blog. In 2007, a 13 year-old girl named Megan Meier committed suicide after receiving a message via MySpace from another user who claimed to be a teenage boy.[17] The investigation of the suicide later revealed that the user who suggested to Meier that she kill herself was not a teenage boy, but an identity fabricated by Lori Drew, the mother of one of Meier's former friends.[18] After the case became a media sensation, a blog titled "Megan Had It Coming" appeared on a popular blog-hosting site.[19] The author of the blog, supposedly one of Megan's classmates, wrote that the deceased girl was a "drama queen" and that Drew could not be blamed for Meier's death.[20] Later, the author of the blog claimed to be Lori Drew, a claim that turned out to be false.[21] Again, the consequences were harmful in very real terms. First, Meier's family suffered the indignity of having their deceased daughter's name tarnished. Second, after the author fraudulently claimed to be Lori Drew, the Drew family was flooded with phone calls and bricks were thrown through their windows.[22] Lori Drew's legal defense was also

12. Mathias Schwartz, *The Trolls Among Us*, N.Y. TIMES MAG., Aug. 3, 2008, at 24, 26–27.

13. *Id.*

14. *Id.*

15. *Id.* at 26.

16. *Id.*

17. *Schwartz, supra* note 12, at 26–27.

18. *Key Events in the Megan Meier Case*, USATODAY.COM, May 15, 2008, http://usatoday30.usatoday.com/tech/products/2008-05-15-1838288037_x.htm.

19. Schwartz, *supra* note 12, at 26.

20. *Id.* at 26–27.

21. *Id.* at 27.

22. *Id.* at 26.

made more difficult by the existence of a blog where the author purported to be a defiant, unrepentant Drew.[23]

By comparison, trolling attacks that fit Kim's "online insults" category cause the same types of harms as cyberdeception but involve totally different behaviors. For example, in 2007, the *Washington Post* ran a story about the web forum AutoAdmit that created a scandal at Yale Law School.[24] The paper conducted several interviews with female law students who chose to remain anonymous for fear of online reprisals from Internet trolls.[25] The story detailed how anonymous classmates of theirs at Yale were using AutoAdmit to post personally-identifying information about the subjects of the story without their permission, along with sexually abusive language directed at them.[26] Posts on AutoAdmit also openly criticized the women's intelligence, qualifications, and capabilities as law students.[27] Again, the women suffered real injuries. One woman in the story reported that she had not received any job offers after being the subject of the AutoAdmit trolling attack.[28] Another said that she no longer went to the gym because the website encouraged users to take pictures of her.[29] This type of trolling attack produces the same types of real-world harms as those involving cyberdeception; however, the specific behaviors that cause the harm are different.

C. What Internet Trolling Behavior Needs Regulation?

The Internet trolling community is difficult to define, much less regulate, because trolls are obsessive about maintaining their anonymity. Due to their close association with hacker communities,[30] trolls tend to be savvy Internet users and much more adept at protecting their own individual privacy than ordinary Internet users. Also, since

23. *MySpace Mom Linked to Missouri Teen's Suicide Being Cyber-Bullied Herself*, FOXNEWS.COM (Dec. 6, 2007), http://www.foxnews.com/story/0,2933,315684,00.html.

24. Ellen Nakashima, *Harsh Words Die Hard on the Web*, WASH. POST, Mar. 7, 2007, at A1, A9.

25. *Id.* at A1.

26. *Id.*; *see also, e.g.*, Kathryn E. Swisher, *The AutoAdmit Scandal and Legal Remedies for Online Victimization*, 17 PERSP. 10, 10 (2009).

27. Nakashima, *supra* note 24, at A1.

28. *Id.*

29. *Id.* at A9.

30. Generally speaking, a "hacker" refers to "a person who illegally gains access to and sometimes tampers with information in a computer system." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 559 (11th ed. 2005). By contrast, a "troll" is defined as either "a deliberately provocative online posting intended to incite an angry response" or "a person who submits a deliberately provocative posting." *Troll Definition*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/english/troll—2 (last visited Nov. 16, 2012).

Internet trolling activity promotes, or even requires, group harassment, it makes sense in most cases to define trolls as a community. Viewed through this prism, trolls generally can be defined as loosely connected groups of individuals who associate on highly unregulated and unmoderated message boards.[31] The best example of a trolling-friendly Internet forum is the notorious "/b/" forum on the Internet site 4chan.com, which has served as a launching point for several infamous trolling attacks.[32] In one example, a trolling meme that may have originated on a 4chan thread developed into a protracted, organized attack on former model Charlotte Dawson.[33] Trolls flooded Dawson's twitter account and e-mail inbox with vicious invectives, calls for her to kill herself, and grotesque images.[34] After weeks of the online harassment, Dawson attempted suicide.[35] The /b/ forum self-regulates (with only limited success) by prohibiting child pornography, the posting of personal information, and open calls to disrupt the function of other websites or online businesses.[36] Beyond that, there are few rules or definitions of what will disqualify a participant.[37] This environment fosters an "anything goes" ethos, which functions to create a hothouse where participants constantly encourage each other to push the envelope of posted comments as well as the language and tenor of the conversation.

In addition to these forums, trolling communities host and promote websites that venerate the most extreme and notorious trolling attacks. Websites such as Encyclopedia Dramatica[38] contain boastful first-person accounts of online trolling endeavors for other members of the community to view and read.[39] For example, the so-called "Fortuny Experiment" involved a member of an online trolling community who proudly posted the results of a bogus adult personal ad, including photographs and phone numbers of respondents, on Encyclopedia

31. *See, e.g.*, *Rules of the Internet*, KNOW YOUR MEME, http://knowyourmeme.com/memes/rules-of-the-internet (last visited Nov. 10, 2012).

32. Schwartz, *supra* note 12, at 24, 26.

33. Jenna Sauers, Next Top Model *Judge Hospitalized after Twitter Bullying Leads to Suicide Attempt*, JEZEBEL (Aug. 30, 2012, 3:30 PM), http://jezebel.com/charlotte-dawson-twitter/.

34. *Id.*

35. *Id.*

36. *See Rules*, 4CHAN, http://www.4chan.org/rules (last visited Nov. 10, 2012).

37. It is worthwhile to note that the first moderation rule for the /b/ forum is "ZOMG NONE!!!1." *Id.*

38. ENCYCLOPEDIA DRAMATICA, (Nov. 14, 2012), https://encyclopediadramatica.se/Main_Page.

39. Schwartz, *supra* note 12, at 27.

Dramatica,[40] from which it spread to the Internet at large. These sites provide not only approval to trolls for their actions, but also serve as models to other trolls who might seek to launch their own hurtful memes.

D. The Role and Importance of Lulz

The concept of "lulz" is another important but difficult to define aspect of trolling behavior. Lulz might be described as a successful attempt to mock or demean the target of an attack.[41] A more practical way to understand lulz is that they are the peer-given rewards for a successful trolling venture. In other words, trolls use lulz to keep score.[42] In form, lulz are no different than any other peer-based reward, such as congratulations from co-workers, which bolster one's reputation. A distinguishing characteristic of lulz, however, is that because trolls seldom seek to gain financially from their attacks, lulz have become their central incentive. In place of financial interests, lulz have become a form of anti-currency. In the general absence of opportunities for commercial gain from trolling attacks, the prospect of acquiring lulz, and the accompanying infamy, has become a powerful incentive. One anonymous troll has described the motivational power of lulz in trolling communities as: "1. Do whatever it takes to get lulz. 2. Make sure the lulz is widely distributed. This will allow for more lulz to be made. 3. The game is never over until all the lulz have been had."[43]

Finally, these attacks bear another important feature: The targets are frequently chosen in an arbitrary fashion. The only trait that the targets of trolling attacks truly share is that some feature of the target has struck an individual troll or a troll community as amusing. In one example, a notorious trolling attack started with the suicide of a teenage boy.[44] Some Internet trolls found a reference on the boy's MySpace page to a lost iPod and, in the hothouse of trolling forums, it became settled that the lost iPod was the cause of the boy's suicide. Soon after this discovery, the boy's parents were bombarded with phone calls, e-mails and letters, many with images of the dead child as an iPod-clutching zombie or other profane, mocking messages.[45]

40. *The Fortuny Experiment*, ENCYCLOPEDIA DRAMATICA, https://encyclopediadramatica.se/RFJason_CL_Experiment (last visited Nov. 14, 2012).

41. *See* Schwartz, *supra* note 12, at 26.

42. *Id.*

43. *Id.*

44. *Id.* at 24–26.

45. *Id.* at 26.

Prior to the attack, nothing connected the deceased child or his family with the trolling community that launched the attack. Rather, his online postings prior to his suicide were simply determined to be suitable material for a large-scale trolling attack. This distinguishes trolling attacks from other forms of cyber-bullying where the victim generally knows the individual perpetrator in the "real" world.

E. The Harms Associated with Lulz Trolling Attacks

Lulz trolling attacks are a cause for legal attention because they possess several harmful attributes. First, they have obvious potential to inflict enormous reputational and emotional injury, as demonstrated by the examples mentioned above. The malicious nature of the content, combined with the accessibility of the Internet, creates vast potential for harming the targets of trolling attacks. In fact, the explicit intent of lulz trolling is to harm targets as publicly as possible. In the lulz community, there is a clear relationship between the amount of harm and pain caused by the attack and the degree to which the attacker is lauded and celebrated within his or her community. Damage to reputation and public embarrassment are the actual ends for many trolling attackers. Therefore, the social incentives driving these trolling communities push the behavior to be more and more malicious, arbitrary, and harmful.

Second, the arbitrary way that trolls select targets makes the need for regulation more compelling. Frequently, as in several of the cases above, the targets have no contact with their attackers prior to the launch of the attacks. The capricious manner in which targets are selected seems to be a central aspect of the enjoyment that Internet trolls derive from their actions. The lulz phenomenon was described by one anonymous troll as "watching someone lose their mind at their computer 2,000 miles away while you chat with friends and laugh."[46]

Third, the frequency of malevolent Internet attacks appears to be rising. While there are no hard statistics on how often harmful trolling attacks occur to American citizens, British authorities report that in 2011 they investigated over 400 trolling attacks.[47] Additionally, some for-profit websites have made use of trolling tactics as part of their business ventures. For example, the adult website isanyoneup.com solicits website users for submissions of sexually explicit photos that were

46. *Id.*

47. Helen Turner, *Police Investigate Almost 400 Online 'Trolling' Attacks in 2011*, WALES ONLINE.CO.UK (Jan. 3, 2012), http://www.walesonline.co.uk/news/wales-news/2012/01/03/police-investigate-almost-400-online-trolling-attacks-in-2011-91466-30049563/.

originally part of private communications.[48] The website publishes the photos, along with the Facebook profiles of the subjects of the pictures, with abusive and sexually explicit commentary.[49] The rise in the number of trolling attacks combined with the new potential for financial gain from trolling behavior make a compelling case for immediate and effective regulation.

II. Present Laws are Ill-Equipped to Regulate Trolling Attacks

The rise in the number of trolling attacks and the brazenness with which they are carried out demonstrates the insufficiency of the current legal framework to deal with trolling attacks. As will be discussed in more detail below, current laws are inadequate in several ways. First, the scope and coverage of most state laws that could apply to trolling attacks are usually insufficient to address the actions of online trolling communities. Second, the penalties—even the criminal penalties—associated with cyberbullying and cyber harassment are insufficient to deter trolling attacks. Finally, the civil causes of action available to the victims of trolling attacks do not adequately cover the victims' injuries.

Compounding the problem is that tort law is presently unable to provide civil remedies to the victims of trolling attacks. The law of privacy torts developed during an era that did not anticipate the threats to privacy that the Internet poses.[50] As a result, the privacy torts, as presently understood, will not support a plaintiff's cause of action even when a plaintiff's injuries are significant.[51]

A. Criminal Statutes

Criminal statutes regarding harmful online behavior generally fall into three categories: cyberharassment statutes, cyberstalking statutes and cyberbullying statutes. None of these types of criminal statutes, however, squarely addresses the problems posed by trolling attacks.

48. Alex Morris, *The Most Hated Man on the Internet*, ROLLING STONE, Oct. 11, 2012, at 44.

49. *Id.*

50. Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 195 (1890) (discussing the need for the law to recognize a right to privacy and the imposition of liability in tort for these and other types of invasions of privacy).

51. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1809–10 (2010) (discussing the need for updated privacy tort law to tackle the information age's privacy injuries).

1. Scope and Coverage

The first and largest problem with present criminal statutes is that generally they fail to cover the behavior of online trolling communities.

Thirty-three states and one U.S. territory have stalking statutes that include language applicable to online behavior.[52] The vast majority of cyberstalking statutes, however, are traditional stalking statutes updated to include stalking behavior that uses computer or cellular technology. The behaviors targeted by these statutes are threatening words or actions, unwanted surveillance of a target, or both. Florida's cyberstalking statute provides an excellent example.[53] Florida's criminal stalking statute has been revised to include "credible threats" communicated through electronic means.[54] The statute defines a "credible threat" as one that,

> places the person who is the target of the threat in reasonable fear for his or her safety or the safety of his or her family members or individuals closely associated with the person, and which is made with the apparent ability to carry out the threat to cause such harm.[55]

Since the targets of trolling attacks are not acquainted in any "real" way with the perpetrators of the attacks, there is usually no conduct that would qualify as a "credible threat" under the statute. Similarly, while many of the attacks merely involve the creation or dissemination of harmful, taunting images or video memes, they rarely involve specific credible threats to the subject's safety. As a result, state cyberstalking statutes nearly always fail to reach the actions of trolling communities. When they do, it is by virtue of a fortunate coincidence that some aspect of the statute can address some feature of a specific attack. Florida's cyberstalking statute is also illustrative of this point in that the statute is densely written and intended to cover a wide range of behaviors but incapable of addressing behaviors such as posting and reposting of intentionally disturbing or grotesque images designed to inflict harm upon a target selected at random.[56] For example, imagine a trolling attack in which a subject receives 100 obscene or harmful messages. Of those 100 messages, two contain a

52. *State Cyberstalking and Cyberharassment Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx (last updated Nov. 16, 2012) [hereinafter *Cyberstalking & Cyberharassment Laws*].

53. FLA. STAT. ANN. § 784.048 (West 2012).

54. *Id.*

55. *Id.*

56. *Id.*

specific, credible threat. A state cyberstalking statute would likely cover only two of the messages, even if the other 98 messages were more obscene or injurious.

The recent crop of cyberbullying statutes is just as ineffective for combating trolling attacks as the cyberstalking statutes. Cyberbullying statutes were written to combat online behavior that facilitates or exacerbates real-world bullying problems.[57] All state cyberbullying statutes limit their language to address behavior in schools by referring to "students," or "pupils."[58] By limiting the scope of the statutes to apply to schoolchildren where there is a pre-existing connection between the perpetrator and victim, the plain language of the cyberbullying statutes makes them almost completely incapable of addressing trolling attacks.[59]

State cyberharassment statutes come closest to addressing the problems posed by trolling attacks. Most of these statutes still fall far short of being an effective tool against these acts. Like the cyberstalking statutes, a majority of the cyberharassment statutes are mere additions of language to existing harassment statutes to include computers as a means by which a person can engage in harassing behavior. State harassment laws that address electronic or telephonic communication are aimed primarily at obscene or harassing phone calls, lewd e-mails targeted at specific people, or threats of extortion.[60] These statutes, however, are targeted at vastly different conduct than the online harassment in which trolling communities engage. A good example of this type of cyberharassment statute is North Carolina's.[61] North Carolina made it illegal to place phone calls that include lewd or profane language, threats to the target or his or her family, or harassment for any reason, regardless of whether a conversation takes place.[62] Tacked onto the end of a list of specifically prohibited telephone practices is an inclusion of computers as a potential means for the prohibited course of conduct.[63] These types of statutes are insufficient to address the harms of trolling attacks because, whereas harassment statutes generally require that the behavior be directly targeted at a specific

57. *Cyberbullying*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/educ/cyberbullying.aspx (last visited Nov. 16, 2012).

58. *Id.*

59. *Id.*

60. *See, e.g.*, IOWA CODE § 708.7 (2011); VA. CODE ANN. § 18.2-152.7:1 (West 2000); WIS. STAT. § 947.0125 (2011).

61. N.C. GEN. STAT. § 14-196(a) (2012).

62. *Id.*

63. *Id.* § 14-196(b) (2012).

person, many trolling attacks are the mere circulation of taunting or offensive images or computer-altered images. Many subjects of trolling attacks find out they have been targeted only once the circulation of the attack reaches a certain level. Said another way, while nearly all trolling attacks have victims, not all trolling attacks have *targets*. As a result, laws requiring or identifying a specific target are not effective tools for dealing with trolling attacks.

Moreover, the harms caused by online harassment necessarily differ from the "real world" harassment imagined by normal harassment laws. In their present form, cyberharassment laws only address the types of online harassment that have some real-world corollary. For example, the harassment described by several state statutes is aimed squarely at spam e-mail.[64] Texas' cyberharassment statute specifically covers e-mail messages transmitted to a recipient without consent when the sender intends to defraud the recipient.[65] Others, like anti-hacking laws, require an unauthorized invasion into a password-protected area.[66] As a result, despite being more Internet-savvy, these statutes are unable to address the type of trolling attacks in which an attacker takes on a false identity in order to solicit embarrassing materials from an unsuspecting person. These statutes also fail to reach the more common attacks where a photograph or image is circulated or altered in order to make it into an intentionally harmful taunt designed to belittle the subject.

2. Insufficient Penalties

The penalties associated with state criminal statutes, as presently constructed, are not a sufficient deterrent. Of the 38 states with cyberharassment statutes, all but four strictly classify cyberharassment as a misdemeanor.[67] Similarly, a strong majority of state cyberstalking statutes classify cyberstalking as a misdemeanor unless there is an aggravating factor such as a violation of probation, a restraining order, or another court order.[68] This presents two problems. First, the punitive weight of a misdemeanor conviction is a totally insufficient deterrent. Considering the amount of harm that some of these attacks have inflicted upon their subjects and victims, punishment by fines or mini-

64. *See* TEX. PENAL CODE ANN. § 33.07 (West 2012).

65. *Id.*

66. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

67. *See Cyberstalking & Cyberharassment Laws*, *supra* note 52 (follow link to each states' website to see individual statutes).

68. *Id.*; *see also, e.g.*, MO. ANN. STAT. § 565.225 (West 2012).

mal jail time is insufficient. Second, because these communities operate in secret and because members carefully protect their identities, the investigative burden is fairly high. Because of these burdens, misdemeanor convictions provide insufficient incentives for state and local jurisdictions to invest time and resources prosecuting members of trolling communities. Members of trolling communities have little reason to fear prosecution and even less reason to fear stiff criminal penalties if they are prosecuted.

3. Drawbacks of Good Criminal Statutes

The foregoing critique of present state law approaches via criminal law does not mean that there are no state criminal statutes capable of addressing trolling attacks. Michigan's cyberharassment law makes it a felony for any person to post anything online without consent of the victim when:

> (a) The person knows or has reason to know that posting the message could cause 2 or more separate noncontiguous acts of unconsented contact with the victim.
>
> (b) Posting the message is intended to cause conduct that would make the victim feel terrorized, frightened, intimidated, threatened, harassed, or molested.
>
> (c) Conduct arising from posting the message would cause a reasonable person to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested.
>
> (d) Conduct arising from posting the message causes the victim to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested.[69]

This language appears to apply to the types of online harassment perpetrated by trolling communities. In addition, subjecting violators to a felony conviction suggests that the Michigan legislature realized the potential severity of trolling attacks. However, even a law as extensive as Michigan's has drawbacks. First, as Michigan's statute demonstrates, criminal statutes that can properly address trolling attacks may require broad language so that they can be applied to the spectrum of malicious circulations of materials and information that can be labeled "trolling attacks." As a result, such laws could unintentionally criminalize benign behavior. For example, imagine a scenario where person A sends out a large e-mail invitation to a birthday party for her friend B. A includes in the e-mail somewhat embarrassing photos of B from previous parties or excursions. If B were offended, harassed, or embarrassed enough *and* two or more e-mail recipients were to reply

69. MICH. COMP. LAWS ANN. § 750.411s (West 2012).

to everyone on the e-mail, including B, with pithy remarks about the photos, a jury could find that A violated the statute and A could be convicted of a felony.

Also, while making a violation of the act a felony provides a stronger deterrent for would-be trolls, the cost and labor of investigating these crimes may prove to be too much for any jurisdiction to ever prioritize. Prosecution and enforcement of even strong laws, like Michigan's, are still subject to the vagaries of the local prosecutor's office. Moreover, because the perpetrators of trolling attacks are loosely associated Internet users, they may not all be located within a single criminal jurisdiction. This dispersion could dramatically increase the time and cost burdens on prosecutors. As a result, victims of these attacks may never receive compensation for their injuries and also may never get the satisfaction of seeing the perpetrators convicted.

B. Privacy and Tort Approaches

Tort law offers several advantages over criminal law in addressing the harms of malicious trolling attacks. First, as referenced above, civil remedies may compensate victims directly for the harms of the attacks. Second, in cases of community-based "viral" attacks that consist of a high volume of individual images or files posted or circulated with varying levels of malice,[70] the plaintiff may tailor the pleading to the perpetrators whose conduct caused the most injury. Finally, because of the wide spectrum of behaviors that fall under the mantle of "trolling attacks,"[71] the comparative malleability of tort standards (as opposed to criminal rules) gives fact-finders a good deal of leeway in assessing the harmfulness of online behavior and the resulting injuries.[72]

Despite offering several potential advantages over regulation through criminal statutes, existing tort law, which is designed to compensate plaintiffs for injuries to reputation or for pure emotional distress, fails to address the conduct of Internet trolling attacks. As a result, present tort law is an inadequate tool for regulating or preventing online trolling attacks.

70. *See, e.g.*, *supra* notes 7–29 and accompanying text.
71. *See, e.g.*, *supra* notes 7–29 and accompanying text.
72. *See infra* Part III.A.

1. Privacy Torts

Trolling attacks frequently include features that are invasive to the privacy of the subject or the target of the attack in a non-legal sense. However, many of the most pernicious behaviors associated with trolling attacks fall outside the bounds of the four traditional privacy torts: Intrusion into seclusion; misappropriation; public disclosure of private facts; and false light. As a result, invasion of privacy claims frequently fail to provide relief to those who have been harmed by Internet trolling attacks.

Restatement (Second) of Torts section 652B defines the tort of intrusion into seclusion: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[73] Like the other privacy torts, the development of intrusion as a tort did not anticipate the invention of the Internet. As a result, there are few decisions that specifically address Internet trolling and case law addressing comparable non-Internet behavior is similarly unhelpful to plaintiffs. In *Stilson v. Reader's Digest Association*,[74] a California court of appeal held that unsolicited mailings do not constitute an intrusion.[75] A Florida court of appeal addressed a pre-Internet age prank comparable to a proto-trolling attack in *Harms v. Miami Daily News, Inc.*[76] In that case, as a prank, a newspaper published plaintiff's phone number attached to the statement: "Wanna hear a sexy telephone voice? Call ———— and ask for Louise."[77] The plaintiff, who was actually named Louise, was flooded with unsolicited and objectionable telephone calls.[78] The court declined to state whether the mere act of publishing the number was an intrusion.[79] Rather, it held that the question of whether or not the conduct was sufficiently "objectionable" was a question for the jury.[80]

Applying these notions to online trolling attacks is not clearly beneficial to plaintiffs. Both *Stilson* and *Harms* conclude that being the recipient of unwanted—and in the case of the *Harms* plaintiff, highly objectionable—communications does not give rise to a cause of action

73. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
74. 104 Cal. Rptr. 581 (Ct. App. 1972).
75. *Id.* at 581.
76. 127 So. 2d 715 (Fla. Dist. Ct. App. 1961).
77. *Id.* at 716.
78. *See id.*
79. *Id.*
80. *Id.* at 718.

for invasion of privacy as a matter of law.[81] In addition, *Harms* appears to preclude the idea that circulating semi-public information to a wider audience for purposes that are outside the scope of the original circulation is an intrusion as a matter of law.[82] Many trolling attacks involve either circulating an image of a subject to a wider audience than the subject originally intended or flooding a target with unwanted communication, or both. As a result, the tort of intrusion into seclusion seems to be historically unavailable to plaintiffs harmed by trolling attacks.

The privacy tort of appropriation is tailored in a similarly poor manner as applied to trolling attacks. Restatement (Second) of Torts section 652C states: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[83] Appropriation does not apply to trolling cases for two reasons. First, it fails to address trolling cases in which there is no appropriation of the plaintiff's image or likeness. Second, a more difficult hurdle is the requirement that the defendant's appropriation of the plaintiff's image or likeness benefit the defendant in some way. This requirement is generally understood to be the acquisition of a pecuniary interest. Currently only four states, New York, Oklahoma, Utah, and Virginia go so far in their statutory language as to explicitly require use "for advertising or the purposes of trade."[84] It is not clear that trolling attacks that use the image of the plaintiff do so in order to confer sufficiently concrete benefits upon the perpetrator. For example, in the notorious "Fortuny Experiment" trolling attack, the defendant took images of men responding to advertisements for sex on Craigslist and published them.[85] However, the defendant Fortuny did not receive any pecuniary or other concrete benefit by doing so.[86] While the plaintiff could have conceivably argued that the defendant did benefit through the approval of his peers as measured in lulz,[87] the alleged benefit of lulz is so far removed from traditional notions of benefit in appropriation cases that it would be a novel argument, to say the least.

81. *See* Stilson v. Reader's Digest Ass'n, 104 Cal. Rptr. 581, 583 (Ct. App. 1972); *Harms*, 127 So. 2d at 718.

82. *See Harms*, 127 So. 2d at 718.

83. RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1965).

84. *Id.* § 652C, Reporter's Note on § 652C (1981).

85. Schwartz, *supra* note 12, at 26.

86. *Id.*

87. *See supra* Part I.D (explaining the concept of "lulz").

The tort of public disclosure of private facts is covered by Restatement (Second) of Torts section 652D:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[88]

Comment (b) of section 652D enumerates the greatest barrier for this tort: The courts' position that the rule "applies only to publicity given to matters concerning the private, as distinguished from the public, life of the individual. There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public."[89] This requirement would bar any claim seeking recovery for a trolling attack that involves the wider circulation of images or materials than the target of the attack originally posted on the Internet. The problem this poses is best illustrated by a hypothetical. Person A posts a picture of himself on a social networking or photo-sharing site so his friends can view it at their leisure. Sometime thereafter, a trolling community finds the photo amusing for whatever reason and starts adding its own abusive commentary or creating derivative images that are insulting to Person A. Eventually, the trolling attack "goes viral" and Person A's image is now viewed by countless users, usually under unflattering circumstances and accompanied by abusive or vulgar commentary. In this hypothetical, the public disclosure of private facts tort is not available to Person A as a cause of action because he made the original image public by posting it on the first website.

A recent California case dealt with the source of an image that led to a trolling attack. *Catsouras v. Department of the California Highway Patrol*[90] addressed the conduct of two California Highway Patrol ("CHP") officers who disseminated the image of a decapitated teenage girl from a traffic accident scene to friends and family as a Halloween joke. The images found their way onto the wider Internet where they were picked up by trolling communities.[91] The family then found out about the leaked pictures after being flooded with e-mails from trolls seeking to make the "lulziest" post.[92] The court held that the family could maintain an action against the CHP officers who origi-

88. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).
89. *Id.*
90. 104 Cal. Rptr. 3d 352 (Ct. App. 2010).
91. *See id.* at 357–58.
92. *See id.*

nally leaked the post, but did not address the subsequent actions of the trolls themselves.[93] Therefore, at present, relief under this theory of invasion of privacy is only available to the victims of trolling attacks when the material is not originally circulated by the victim. Liability also appears limited to individuals who first circulated the images without authorization, rather than the subsequent trolls or trolling communities.[94]

Finally, the tort of false light presents the same kinds of tailoring problems as the other privacy torts. Restatement (Second) of Torts section 625E assigns civil liability to an actor who publicizes information that places a plaintiff in a false light when the false light would be highly offensive to a reasonable person, and "the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[95] Comment A to Section 652E limits the applicability of the false light to disclosures of private information that necessarily include some kind of falsehood about the plaintiff.[96] Therefore, on the one hand, the tort may include some behaviors associated with trolling attacks such as the circulation of an altered image designed to impute some falsehood about the subject's character, history, or beliefs. On the other hand, a wider spectrum of other behaviors, such as mere circulation of an embarrassing photo or large scale circulation of vulgar commentary about a targeted woman's body, are not addressed by this tort. Like the cyberstalking and cyberharassment statutes discussed earlier, some but not all behaviors associated with trolling attacks may be covered by this tort. As a result, the scope and coverage of this one tort are insufficient to regulate a phenomenon that encapsulates such a broad range of behaviors.

C. Intentional Torts

Intentional torts present some of the same problems as privacy torts. Restatement (Second) of Torts section 46 assigns liability to a person "who, by extreme and outrageous conduct, intentionally or recklessly causes severe emotional distress to another[.]"[97] That person is subject to liability for such emotional distress and if bodily harm

93. *Id.* at 375.
94. *See id.* at 374.
95. RESTATEMENT (SECOND) OF TORTS § 652E (1977).
96. *Id.* § 652E cmt. a.
97. *Id.* § 46 (1965).

to the other results from it, for such bodily harm.[98] However, the authorities are unanimous that not every assault on a target's emotional well-being or prevailing notions of decency will sustain a claim.[99] "There is no occasion for the law to intervene in every case where some one's feelings are hurt. There must still be freedom to express an unflattering opinion, and some safety valve must be left through which irascible tempers may blow off relatively harmless steam."[100] As a result, the line between what is actionable as an intentional infliction of emotional distress and what falls to pieces under the premise of *de minimis non curat lex*[101] is frequently hazy and difficult to identify.

Additionally, in the instances where the trolling conduct is sufficient to support a claim for intentional infliction of emotional distress, the scope and coverage problems that hamper the effectiveness of false light and cyberharassment statutes as a regulatory tool for Internet trolling also limit the effectiveness of intentional infliction of emotional distress. Imagine the same trolling attack proposed earlier that consists of 100 messages. Two just happen to fall under a state cyberharassment statute, five more contain a falsehood that could support a claim for false light, and three more are extreme and outrageous enough to support a claim of intentional infliction of emotional distress. A plaintiff would still face a scenario where only 10% of the conduct that injured him could provide him with any form of compensation and 90% of the bad actors involved in the attack would not incur any legal risk for their behavior. In this way, intentional infliction of emotional distress, even when sufficient to address some trolling behaviors, is insufficient as a regulatory tool.

D. Defamation

While trolling attacks are highly vulgar, offensive, or insulting, they frequently do not fit our present legal definition of defamation. In the broadest terms, defamation is the non-privileged publication of a false statement that tends to injure the reputation of the plaintiff.[102] The primary pitfall is that while a claim for defamation requires a specific falsehood, trolling attacks frequently do not include false statements. Rather, their effectiveness lies in taking true statements and

98. *Id.*
99. *Id.* § 46 cmt. d.
100. *Id.*
101. "The law does not concern itself with trifles." BLACK'S LAW DICTIONARY 496 (9th ed. 2009).
102. *See* RESTATEMENT (SECOND) OF TORTS § 558 (1977).

placing them in different contexts, or taking semi-public information and distributing it to a much broader audience. For example, the primary substance of the trolling attack relating to the claim in *Catsouras* was the intentional posting of the leaked photos in places where unsuspecting Internet users would happen upon them and the creation of a fake MySpace tribute site to the deceased girl.[103] Similarly, the substance of the Fortuny Experiment involved the intentional publication of photographs, phone numbers, and private, sexually explicit e-mails to a larger audience.[104] This illustrates the difficulty that the law of defamation faces as a tool for regulating this online behavior. Defamation requires a falsehood, which many of the vilest trolling attacks lack.

III. Proposed Solution

The randomness of the way trolls select their victims makes everyone who uses the Internet in a conventional way a potential victim. The harms caused by trolling attacks can be severe, and the limited statistics on the subject show that these attacks are increasing.[105] As a result, the perpetrators of these attacks should face some significant legal risks if they choose to engage in these activities. Most behaviors that compose trolling attacks however, are too varied to squarely fit into existing criminal laws or into the elements of existing tort law. So how should the law go about addressing this disturbing micro-trend of Internet usage?

A. Guiding Principles

The legal approach to trolling attacks should be governed by several principles. First, it should provide sufficiently severe penalties to raise the risk associated with starting or exacerbating a trolling attack. Second, it should be able to provide relief to plaintiffs proportional to the injuries they have suffered. Third, the approach should not chill online speech more than is absolutely necessary. Finally, the approach needs to be broad enough to cover the wide variety of behaviors that

103. Reynolds Holding, *Family Can Sue Calif. Highway Patrol for Letting Daughter's Accident Photos Spread Online*, ABC NEWS (Feb. 2, 2010), http://abcnews.go.com/TheLaw/nicole-catsouras-fatal-accident-photos-web-family-sue/story?id=9731639#.UJ6wauOe-I2; *see also* Greg Hardesty, *Family Gets $2.4 Million Over Grisly Crash Images*, ORANGE COUNTY REGISTER (Jan. 30, 2012), http://www.ocregister.com/articles/family-337967-catsouras-nikki.html.

104. Schwartz, *supra* note 12, at 26.

105. *Cf.* Turner, *supra* note 47.

comprise trolling attacks and to be adaptable to future techniques adopted by trolling communities and individual trolls.

Despite the shortcomings of the current tort law described above, it provides the best avenue for regulation for several reasons. Prosecution of trolls by way of criminal law requires a willingness of the authorities and prosecutors to investigate and prosecute bad actors. By contrast, tort law allows injured parties to identify the most injurious behaviors and tailor pleadings accordingly. Also, while new legislation that provides either new criminal penalties or new civil remedies can limit future applicability, new tort principles have historically demonstrated the ability to adapt to new and different social circumstances. An example of just such an adoption was the use of strict liability for defectively manufactured products in response to the development of mass-produced goods.[106] In addition, existing doctrinal safeguards already ensure that the limitations on speech via a tort scheme will not chill speech any more than is constitutionally permitted.[107] Tort law also allows injured parties to seek adequate relief and for fact-finders to weigh all relevant factors in determining the remedy, which provides much-needed flexibility in the context of trolling attacks.

B. Updating Public Disclosure of Private Facts

Courts should interpret the doctrine of public disclosure of private facts to apply to the rise of trolling communities and the attacks in which they engage. A plaintiff who is injured in a trolling attack should be able to prevail under this theory of invasion of privacy upon an affirmative showing that:

(1) The defendant circulated private or semi-private images or material online without consent of the author or subject of the material; and

(2) The defendant knew or should have known that his actions would expand the circulation of the online material beyond the scope of its intended circulation; and

(3) The defendant knew or should have known that the circulation of the material would be offensive or otherwise harmful to the subject of the circulated material; or

(4) The defendant circulated the material in a manner intentionally designed to harm the target or subject of the material or with reckless disregard to the harm the circulation would likely cause.

106. Francis J. O'Brien, *The History of Products Liability*, 62 TUL. L. REV. 313, 322 (1988).
107. *See* N.Y. Times v. Sullivan, 376 U.S. 254, 300 (1964).

C. Definitions and Benefits

The most dramatic departure from the existing tort of public disclosure is the elimination of the requirement that the disclosed materials are strictly private. As discussed earlier, the traditional approach to public disclosure bars liability to individuals who make their own information public. In the offline context, this made sense. It was contradictory for a plaintiff to take a public action and then raise an issue about the number of people that saw the act. As online posting, sharing, and storage of materials increasingly becomes the norm, the lines between public and private have become less clear. For example, imagine that person A sends an e-mail to three of her friends with photographs from a weekend excursion to Las Vegas. One of the friends, B, places one of the photographs—a picture of A in a mildly embarrassing pose—on her Facebook page and has less stringent privacy settings than A. From there, an Internet troll finds some aspect of the picture amusing and, in short order, the picture, accompanied by vulgar insults and commentary, goes viral. A loses her job as a result. Under the traditional approach to public disclosure, A would almost certainly be barred from recovery because she had originally e-mailed the photos to the three friends and thus they were no longer "private."

In the second element, the new approach recognizes that many materials posted, stored, and shared online have an intended circulation and it is very hard to keep materials strictly "private" under these circumstances. Private materials have no intended circulation; semi-private materials have a limited intended circulation. This is an important distinction online. Under this approach, the plaintiff must make an affirmative showing of who made up the anticipated audience and how the further circulation was outside the scope of the intended audience. This showing can be made in a variety of ways such as the e-mail recipient list, social network privacy settings, online invitation lists, or password protection. Conversely, if a plaintiff was genuinely cavalier about disseminating their information, a jury could find that the anticipated audience was too nebulously defined and deny a plaintiff seeking to classify materials as "semi-private."

The last change that the new approach adopts is a *scienter*[108] requirement. A defendant must know or should know that his actions would be harmful. This will help to reduce the potential for liability in

108. "A degree of knowledge that makes a person legally responsible for the consequences of his or her act or omission; the fact of an act's having been done knowingly . . . ." BLACK'S LAW DICTIONARY 1463 (9th ed. 2009).

cases of honest mistake or more benign disclosures. Finally, the fourth element borrows the standard of intentional or reckless behavior from the other intentional torts. This is necessary because the core behaviors of trolling attacks and the lulz phenomenon help distinguish between those individuals who conceive or start an attack and those who merely perpetuate an attack.

The adoption of these factors into consideration of public disclosure in the online setting satisfies all the principles set forth above in Part II.A. First, as a tort standard, it will have the flexibility to attach liability commensurate with harm. Second, attaching significance to the broadened circulation of online materials properly recognizes that the harm of these attacks frequently derives not from mere disclosure, but from broadened disclosure to unintended recipients. By attaching liability to the amount that the materials are circulated, this interpretation attaches the risk of liability more proportionally to the harm actually inflicted by trolling attacks. In this way, fact-finders will be able to assign penalties based on the breadth of circulation.

Additionally, the emphasis on circulation is broad enough to include all behaviors of which trolling attacks consist. To illustrate, while there might be great variety in the manner in which the materials of a trolling attack are circulated, trolling attacks all necessarily involve the circulation of the materials in order to effectuate their goals. Therefore, future attacks—regardless of their form—will necessarily fall within the terms of this interpretative standard.

One of the main potential dangers with any regime regulating speech is the possibility that it will apply to more speech than is absolutely necessary. These problems most frequently arise in speech involving public figures. While most of the trolling attacks this proposal seeks to regulate are aimed at private individuals, the attacks are not limited to them. For example, in 2011, the trolling group LulzSec launched a coordinated attack on the Facebook page of Republican presidential candidate Newt Gingrich.[109] While elements of this attack were consistent with the juvenile and occasionally vulgar behaviors of other trolling attacks, some of the content (including the decision to attack a political figure) was entitled to some level of constitutional protection. However, existing protections can be easily applied to this

109. Jeromie Williams, *LulzSec Launches Post South Carolina Primary Trolling Attack On Newt Gingrich Facebook Page*, JEROMIE WILLIAMS EATS THE INTERNET FOR BREAKFAST (Oct. 15, 2012, 4:05 PM), http://jeromiewilliams.com/2012/01/22/lulzsec-launches-post-south-carolina-primary-trolling-attack-on-newt-gingrich-facebook-page/.

standard to ensure that it does not curtail more speech than is constitutional.

The Supreme Court's decision in *New York Times v. Sullivan*[110] provides the proper level of constitutional protection.[111] In *Sullivan*, the Court held that a public figure may not recover civil damages for defamation absent a showing that the defamatory statements were made with actual malice.[112] The Court went on to define actual malice as reckless disregard for the truth of the assertion.[113] Three years later, the Court extended the doctrine of actual malice into the realm of invasion of privacy in *Time, Inc. v. Hill*.[114] In *Hill*, the Court held that the First Amendment barred a public figure from recovering for false light absent a showing of actual malice.[115] The actual malice standard may be applied to the proposed interpretation of public disclosure of private facts. Applying this standard to attacks on public figures would prohibit only known falsehoods or reckless falsehoods. The standard would still permit liability for the intentionally disruptive, the nonsensical, and the juvenile statements that comprise most trolling attacks. This would strike the proper balance between allowing public figures to defend themselves and the First Amendment.

Conclusion

The harms posed by coordinated trolling attacks are too great to ignore. Lulz have provided sufficient motivation to trolls to increase their frequency and potential for harm. Existing criminal statutes do not properly address the problem. In addition, while present tort law can address some of the potential harms, it fails to adequately encompass all the behaviors associated with trolling attacks. The existing framework of privacy torts should be adapted and updated to deal with the threats to privacy and the risk of reputational harm that are posed by trolling attacks. The adaptation should come in the form of a new interpretation of the tort of public disclosure of private facts as it pertains to online conduct. The emphasis should be on the circulation of materials rather than simple disclosure. The actual malice standard contained in *New York Times v. Sullivan* provides sufficient constitutional protections to the legitimate speech aspects of trolling

110. 376 U.S. 254, 302 (1964).
111. *Id.* at 285–92.
112. *Id.* at 279–80.
113. *Id.* at 280.
114. 385 U.S. 374, 387–88 (1967).
115. *Id.* at 384 n.8.

behavior. The First Amendment standard is entirely compatible with—and can be easily overlaid onto—this new approach to public disclosure of private facts. Our legal system already has the proper pieces to compensate victims of malicious online attacks, however, a new approach to privacy torts is needed to bring the pieces together. The adoption of the approach laid out above would be a substantial step in the right direction.